

Running the Matrix: Kerberos Extensions and Owning the Universe

Curtis E.A. Karnow ckarnow@sonnenschein.com www.sonnenschein.com





I Introduction



Disclaimers

- Sun
- All public materials



Outline #1

- Problem with Propriety Protocols and Extensions
 - He Who Owns the Code Owns the Universe
- · Interoperability; open/closed standards
- Example: Kerberos



Outline #2

- · Public law- a balancing of public/private interests
- Undermining balance with proprietary protocols
- · Recent laws (DMCA) further upsetting the balance



II Standards: Open v. Closed (Proprietary)



Standards Link the Net

- Must have standards for interoperability
- · Security standards especially important: every node must

speak same language- each user, client, server and application- must authenticate to each of the others

· Tipping to one standard: The virus effect (client/server)



What are "Open" standards?

- Source published? Licensed? Free?
- APIs disclosed?
- · Public detailed specification?
 - Enough to write to and use?
 - Enough to implement on a different platform?
- · Various levels of interoperability
 - data exchange
 - take advantage of partial or full functionality



Rationale for Closed Standards

- market control
- difficulty with public law- e.g. inadequate IP protection
- · technical frustration/flexibility
- · desire for new features
- skin in the game
- · reaping the rewards of innovation



Dangers of Closed Standards

- Danger in digital network context; implicates control across entire network
- · diminish interoperability, cross platform
- · Switching costs
- · Future in the hands of one entity
- No peer review- bad if we want to avoid security through obscurity



Other Dangers of Closed Standards

 threatens the public law balance- system enforces not necessarily public values but private fiat · increase legal overhead- fights over ownership



Standards Across Markets

- Networked world: standard for one market explodes into neighboring ones, e.g.
 - Hand helds
 - phones
 - content & DRM
 - Servers
 - other web services



Standards "ajar"

- · Proprietary extension of public protocols
- Partially open? Partial disclosure? Disclosed -- but licensed for implementation? Restricted licenses?
- · Confusion, FUD
- · Fertile ground for unintended incompatibility



III Kerberos



Kerberos Encryption Schema

- Example of a public protocol (MIT) that has been subject to proprietary (private) extensions
- · Authentication- cross realm & through series of servers
- Value in context of e.g. digital rights management, network generally
- · No unsecured exchange of passwords (no sniffing)



- client request for credentials made to authentication server (AS)
- [AS = database of "principals" (users, servers) + their secret keys]
- · AS then provides credentials to client, encrypted with secret

key



Kerberos Access Target server

- · Credentials include ticket for access to server & session key
- Ticket used by client to access server. Session key shared by client & server
- · Server, client, user all authenticated to the others





MS Announces Kerberos Support

- "Windows 2000 [uses] the Kerberos Version 5
 authentication protocol ... an <u>open standards</u> protocol"
- <MS Press Release May 9, 2000><emphasis supplied>
- Default authentication protocol for Windows 2000 and XP is Kerberos v.5



Standards Ajar:

Microsoft's Approach (2000)

- Infiltration by privately "owned" patents and 'trade secrets'
- · Various patents, proprietary extensions in the PAC field
 - Note that original MIT implementation of field was intended for vendor definition



MS PAC Implementation

- · MS Security identifiers (SIDs), included in ticket
 - = PAC (Privilege Attribute Certificate)
 - supports user accounts and groups
 - Win Domain controller includes user accounts/machines/groups, directory server, Kerberos KDC [key distribution center] & group policies



PAC & Interoperability

- Open PAC would allow non-MS products to imitate Windows domain controller
- can't replicate functionality of Windows domain controller (as of Aug. 2002)



PAC & Interoperability- The Reports

- [Windows client]-[non-Windows server] "MS Kerberos and UNIX Kerberos interoperates "so long as you're not trying to serve logons to Microsoft client" http://mirrors.sunsite.dk/samba/slides/enterprisesamba.pd
- "Microsoft's implementation... is incompatible with the rest of the Kerberos world..." B. Schneier, <u>Secrets & Lies</u> at 149
- [Non-Windows client]- [Windows server]- unknown



Enforcement of MS' PAC

- · First: Specification confidential/secret
- Then: Specification released- but need to run Windows .exe which presents click-through > promise to treat as trade secret
 - Looks like limited disclosure- ok to inspect but no permission to implement
 - Infinite distribution of trade secret!
- Slash dot leak
- Still, some remark: not enough to implement full MS Kerberos on other platforms



Effects of Windows PAC

- pushes platform (e.g. server, Windows) for interoperability reasons- may not be best
- · pushes related protocol/architecture, e.g.
 - Active Directory

- Passport (single sign on)
- · increased switching costs
- · Security through obscurity



IV Public Law // Private Interest



Public law

- · Protect private property AND supercede private interest
- · 2 components: substantive and procedural
 - Substantive: politics; balancing public v. private-making a bargain--generates the rule of law
 - Procedural: enforcement: the courts, judgesacceptable if law is fair and balanced



Substantive Public Law

- Hard work done in legislatures, politics weighs interests, balancing: encouraging private interest at the right cost to the public, upholding public values
- Most laws balance = limitation of private freedom of action to impose a public benefit
 - Dangerous exception: "Elastic Tape Measure Laws"



Balancing: public values /private rights

- no "illegal contracts" which are against public policy (contract to kill, perhaps gambling debts)
- · zoning, noise regulations
- campaign contribution (limiting first amendment freedom of expression for the public benefit of lessening corruption)
- speed laws



Balancing: public values /private rights:

Most intellectual property laws

 copyright (but protects only against copying & not independent creation, term of years; expression not

- idea; fair use)
- patent (but term of years, narrow protection; disclosure)
- trademark (but nominal "fair" use, first amendment)



Trade Secrets- what balance?

- most dangerous
 - cheap
 - eternal
 - Highly elastic: anything qualifies
 - · No public interest / political balance
 - · [Details later]
 - criminal predicate
- most delicate: leak kills it



Elastic Tape Measure Laws

- · Where the classic model breaks down
 - substantive protection is privately- not publiclydefined-
- and full public procedural law is still available



Elastic Tape Measure Laws: examples

- crime to enter site unless "authorized"- private party defines authority
- · trade secret- anything qualifies
- · contract (license agreement)
 - Although limits: adhesion, against public policy, illegal



Fair use - The Balancing Act

- public right embodied in the copyright act
- · right to use/copy without permission
- can be used to explore and avoid the impact of proprietary protocols and extensions



Establishing Fair Use

- Criticism
- Comment
- · News-reporting
- · Scholarship
- Research
- Teaching
- · Examples are not exhaustive



Fair use: Reverse Engineering

- · includes right to disassemble
- For purpose of e.g. creating interoperable components and code



V Upsetting The Balance

- · Proprietary Extensions
- · New Laws



Proprietary Extensions Upset the Balance

 Use procedural public law- but not to enforce substantive public law but rather broad private interests



Trade Secrets- the Ancient Balance

- · Any leak destroys- so
 - Trade secrets were methods & processes
 - product itself- public



Magic Weapons of Proprietary Extensions

- "Trade secrets" (or other IP) + license agreements = binaries (digital black box) + distribution via license
- Magic!:
 - trade secrets can't be disclosed

- license agreement allows disclosure



Magic Weapon

- Use w/out license = breach of contract; trade secret infringement
- · Enforcement: Both civil and criminal procedural law



Supremacy Fight: Public values or Private contract

- should contractual restrictions against e.g fair use supercede copyright law/fair use?
- · Backdrop: Almost any right can be waived
 - right to counsel, even trial, in a capital case
- Thus: Default: contracts (licenses) always trump
- assumes free choice, no adhesion, when it comes to contracting, ideal market forces



Illusion of Consent

- Switching costs: locked into private standards
- · No negotiations in most s/w licenses



VI New Statutory Threats

- · Digital Millennium Copyright Act
 - bar on reverse engineering re decryption & security systems, hurting fair use
 - can't 'traffic' in anti-circumvention technology
- state "baby" DMCAs
- · Extending term of copyright
- UCITA validation of clickwrap (2 states)
 - Bomb shelters



Statutory Threat: Proposed "US Patriot Act II"

- · "Domestic Security Enhancement Act"
- · criminalizes use of encryption to conceal evidence relating

to any other federal crime

- Copyright is a 'crime'
- many federal crimes, such as terrorism, RICO, fraud (mail & wire) include or overlap w/state laws- most everything is covered
- undermine "fair use," particularly in the context of examining proprietary encryption schemes
- Criminal penalties, risk of suit: if there is any examination of, or use of, encryption



VII Conclusion



Risk of Lock In

- · Rise of network / need for interoperability
- Increasing complex, interdependent functions and standards
- New cases & legislation validating restrictive technology and legal provisions: Magic (trade secrets & licenses)
- · Thus:



All your code are belong to us

- He who owns the protocols owns the network
- E.g. Kerberos: implications for server, directory, single sign on, etc. technologies
- DRM etc. control over content/apps. passes from user to chip maker & s/w developer
- Removal of knowledge from the commonweal, loss of the commons



A call for full public standards /open source?

- · IP is freely licensed
- · fully accessible
- · all platforms
- no restrictions on reverse engineering or copying-fully published specifications and permissions to use/implement

on any platform

· especially in security context



Resources/ Appendix

- Abstract
- · Speaker Biography
- Sites
- Old Kerberos License
- Cases
- · Kerberos Patents





Abstract

The presentation will use the Kerberos encryption schema as an example of a public protocol that has been subject to proprietary (private) extensions. Proprietary protocols are especially dangerous in the digital network context, since control of one protocol can implicate control across the network. A short non-technical outline of the Kerberos system and topology is presented, as well as the means by which the public standard has been infiltrated by certain privately "owned" patents and trade secrets. This leads to a discussion of how public law--intellectual property law (copyright, patent, etc.) -- is used to enforce private interests. Public law--usually the guarantor of a balancing of public and private rights-is used in this context to upset that balance to benefit private control. Fair use, a public right embodied in the copyright act, can be used to explore and avoid the impact of proprietary protocols and extensions; but new laws, such as the Digital Millennium Copyright Act and the proposed anti-terrorism statute "US Patriot Act II" undermine the utility of "fair use," particularly in the context of examining proprietary encryption schemes.

Speaker Biography

Curtis Karnow is a partner at the law firm of Sonnenschein, Nath & Rosenthal, LLP, and a member of the firm's ecommerce, security and privacy, and intellectual property groups. He is the author of Future Codes: Essays In Advanced Computer Technology & The Law (Artech House, 1997), and represents Sun Microsystems in the landmark antitrust case, Sun Microsystems v. Microsoft. His clients have also included Yahoo!, Charles Schwab & Co., Inc., Cisco, Sony Computer Entertainment of America (Playstation), and PGP (Pretty Good Privacy). Mr. Karnow has counseled on public key infrastructure policies, electronic contracting, and digital signatures. Formerly Assistant U.S. Attorney in the Criminal Division, Mr. Karnow's responsibilities included prosecution of all federal crimes, including complex white-collar fraud. from investigation and indictment through jury verdict and appeal. Since then, Mr. Karnow has represented defendants indicted for unauthorized access to federal interest computers; defended against a criminal grand jury investigation into high tech (encryption) export actions; represented clients before federal grand juries investigating alleged antitrust conspiracies and securities violations; brought legal actions against internet-mediated attacks on client networks, and in a state criminal investigation represented a computer professional framed by a colleague in a complex computer sabotage. He has also advised on jurisdictional issues arising out of a federal criminal Internet-related indictment, and advises on liability and policy issues, including interfacing with law enforcement authorities, arising from computer security breaches and Internet privacy matters. He occasionally sits as a temporary judge in the California state court system.

55

Sites Etc.

- · http://www.cybersafe.ltd.uk/
- http://web.mit.edu/kerberos/www/
- http://www.ietf.org/html.charters/krb-wg-charter.html
- http://www.isi.edu/gost/brian/security/kerberos.html

- http://home.xnet.com/~catena/ms-kerberos.shtml
- C. Todd et al, <u>Hack Proofing</u> at 67 et seq. (2001)
- kerberos-request@MIT.edu & info-kerberos@MIT.EDU
- http://www.microsoft.com/windows2000/techinfo/howitwor ks/security/kerbint.asp
- http://slashdot.org/articles/00/05/02/158204.shtml



The Old MS Kerberos License

"Check out the URL:

$\frac{http://www.infoworld.com/articles/en/xml/00/04/28/000428enke}{rpub.xml}$

Essentially, Microsoft have documented the proprietary changes they made to Kerberos 5, but made the changes available in a self extracting executable. Running this .exe gives this click-through license which you must agree to before extracting (NB. I did not agree and the extract terminates). "b. The Specification is confidential information and a trade secret of Microsoft. Therefore, you may not disclose the Specification to anyone else (except as specifically allowed below), and you must take reasonable security precautions, at least as great as the precautions you take to protect your own confidential information, to keep the Specification confidential. If you are an entity, you may disclose the Specification to your full-time employees on a need to know basis, provided that you have executed appropriate written agreements with your employees sufficient to enable you to comply with the terms of this Agreement. You are also permitted to discuss the Specification with anyone else who has downloaded the Specification and agreed to these terms and conditions."



Cases, Etc.

Fair Use and Interoperability

- Sega Enterprises Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992)
- Sony Computer Entertainment, Inc. v. Connectix Corporation, 203 F.3d 596 (9th Cir. 2000)
- Dunn & Bradstreet Software Services v. Grace Consulting,

Inc., 307 F.3d 197 (3d Cir. 2002)

- Deborah F. Buckman, Annotation, Copyright Protection of Computer Programs, 180 A.L.R. Fed 1 (2002)
- David Nimmer, Nimmer on Copyright, volume 4 § 13.05 (D)(4) (2003)

Tightening the Scope of "Fair Use"

Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000)

DeCSS circumvents the CSS protection system and allows CSS-protected motion pictures to be copied and played on devices that lacked the licensed decryption technology. Plaintiffs motion pictures studies sued under the DMCA and enjoined defendants from posting DeCSS and prevented them from linking their site to others that post DeCSS.

Court rejected fair use and 1st amendment arguments, noting that the fair use defenses under the DMCA differ from the fair use defenses under older copyright law. Traditional defenses to copyright infringement, including fair use, are fully applicable only if initial access is authorized. In addition, the DMCA specifically excepts only narrowly defined types of reverse engineering, security testing, good faith encryption research, and certain uses by nonprofit libraries, archives and educational institutions.

Shrink Wrap License

ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996)
Company included a shrink-wrap license in its packaged software of a database of telephone numbers. Defendant purchased a consumer package of the software, but ignored the license restricting its use to non-commercial purposes. The court enforced the terms of the shrink-wrap license.

Court rejected the argument that copyright law preempted contract enforcement. Although the content of the electronic database was not protected by copyright law, it could be protected by contract. In addition, using the software after having had the opportunity to view the license sufficed as consent to the terms of the license.

Additional items

"The Shrink-Wrap License - Is It Really Necessary?" 10 Computer Lawyer # at page 16 (August, 1993). Discusses reverse-engineering as fair use; shrink wrap restriction therefore against public policy

D. Maher, "The Shrink-Wrap License: Old Problems in a New Wrapper" 34 <u>Journal of the CR Soc</u>. (No. 3, April 1987) at 292 (a venerable paper!)

People v. Network Associates Inc. d/b/a McAfee Software (NY Sup. Ct. 2003)(Prohibition on review of software in license is unfair trade practice)

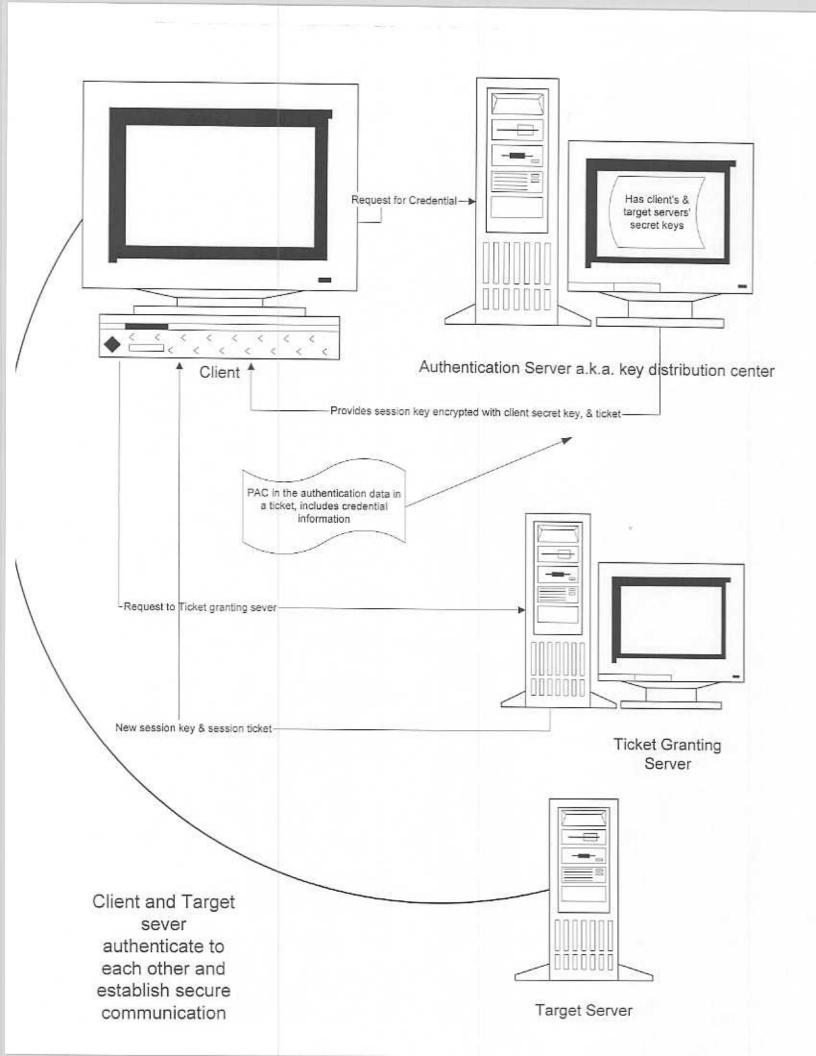
Bowers v. Baystate Technologies Inc., 302 F3d 1334 (Fed. Cir.) & 65 PQ2d 1746 (2003)(Prohibition vs reverse engineering in shrink wrap not preempted by Copyright Act)

Internet Society's statement on Digital Rights Management, http://www.isoc.org/isoc/media/releases/020815pr.shtml



Kerberos related patents

6,536,037 Identification of redundancies and omissions among components of a web based architecture 6,519,571 Dynamic customer profile management 6,473,794 System for establishing plan to test components of web based framework by displaying pictorial representation and conveying indicia coded components of existing network framework 6,427,209 System and method of user logon in combination with user authentication for network access 6,401,211 System and method of user logon in combination with user authentication for network access 6,400,996 Adaptive pattern recognition based control system and method 5,999,711 Method and system for providing certificates holding authentication and authorization information for users/machines 5,757,920 Logon certification



Running the Matrix: Kerberos Extensions and Owning the Universe

Curtis E.A. Karnow ckarnow@sonnenschein.com www.sonnenschein.com

Additional Resources

THE FINANCIAL PAGE PATENT BENDING

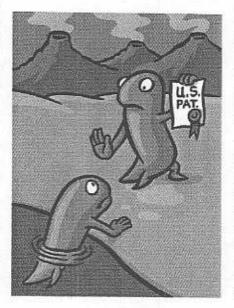
The American newspaper business as we know it was born on September 3, 1833, when a twenty-three-year-old publisher named Benjamin Day put out the first edition of the New York Sun. Whereas other papers sold for five or six cents, the Sun cost just a penny. For revenue, Day relied on advertising rather than on subscriptions. Above all, he revolutionized the way papers were distributed. He sold them to newsboys in lots of a hundred to hawk in the street. Before long, Day was the most important publisher in New York.

One thing that Day did not do was patent any of these innovations. Soon after the Sun appeared, penny papers made their début in Boston and Baltimore; in New York, James Gordon Bennett started the Herald, mimicking the Sun's price and sales methods. By 1840, the Sun and the Herald were the country's two most popular dailies.

This is how American business worked until very recently. Innovators came up with new ways of selling products, handling suppliers, running organizations, or managing information. If the ideas were good, the innovators got rich, but they also got imitated, which made them less rich than they might have been. It was great for everyone else, though. The competition lowered prices and increased quality; the new ideas spread and were improved upon. The mail-order catalogue, the moving assembly line, the decentralized corporation, the frequentflier mile, the category-killer store—none of these radical ideas were patented.

Those were the days. Now the first thing someone with a good notion does is press the government to protect it. Priceline patented its reverse-auction method for selling cut-rate airline tickets. I.B.M. patented a method for keeping track of people waiting in line for the bathroom. Last month, Netflix, a company that runs an online DVD-rental subscription service, got a patent covering, among other things, the way its customers request titles and the way it sends out DVDs. And eBay is now in court appealing a verdict that it infringed on a Virginia man's patent. The crime? Selling auctioned items at a fixed price. What gall.

For most of American history, it was next to impossible to get a patent on what the U.S. Patent and Trademark Office called "a mere method of doing business." A business method was considered to be an idea—selling newspapers in the streets, delivering packages overnight—and ideas of this sort were not patentable. But in July, 1998, the U.S. Court of Appeals for the Federal Circuit did away with that principle. The case, State Street v. Signature Financial, involved software that Signature had written to enable it to administer mutual funds more efficiently. But the court's language



was broad enough to embrace any business process (as long as it was new and "nonobvious" and had a "useful, concrete, and tangible result"). The gates opened, and in the past five years thousands of business-method patents have been granted. One inventive soul won a patent for a system of using pictures to train janitors. Another got one for describing a way to cut hair with both hands.

All patents, of course, stifle competition. That's why inventors like them. But business-method patents have an especially chilling effect, in that novel approaches to commerce can be ruled offlimits to others. What eBay was accused of copying was a concept, not a computer code. As James Boyle, a law professor at Duke, put it, "Under this logic, one could get a patent on the idea of fast food—not a different way to broil the burger but the idea of fast food itself."

Although intellectual-property experts like Boyle have loudly criticized the State Street decision, Congress has shown little interest in doing anything about it. (In fact, lawmakers have proposed bills that would make things even worse, such as allowing sports "techniques" to be patented. Imagine pitchers paying a royalty every time they threw a forkball.) That has left the matter of business-method patents in the hands of patent judges and the staffers at the Patent Office-people who spend most of their time working with patent-seekers, and who are therefore more sympathetic to their interests than to the public's. (Economists call this phenomenon "regulatory capture.") The office says on its Web site that its role is "to grant patents," but surely its role should be to distinguish between innovations that are worth patenting and those that

Americans have traditionally been chary about intellectual-property rights. Thomas Jefferson, who served on the nation's first patent board, wrote, "If nature has made any one thing less susceptible than all others of exclusive property, it is the action of the thinking power called an idea." Although we have always had a vibrant patent system, we've managed to strike a balance between the need to encourage innovation and the need to foster competition. As Benjamin Day, Henry Ford, and Sam Walton might attest, American corporations have thrived on innovative ideas and new business methods, without owning them, for two centuries. In the past decade, the balance has been upset. The scope of patents has been expanded, copyrights have been extended, trademarks have been subjected to bizarre interpretations. Celebrities are even claiming exclusive ownership of their first names (consider Spike Lee's objection to Viacom's cable channel Spike TV). The new regime's defenders insist that in today's economy such vigilance is necessary; ideas are the source of our competitive strength. Fair enough. But you don't compete by outlawing your competition.

—James Surowiecki

Look Here First To Find Vendors Fast.





COMPUTERWORLD An IDG

Home

News

Topics Departments

Services

Subscriptions

Events

You may retrieve this story by entering QuickLink# 27956

► Return to story

Microsoft to offer concessions in EC antitrust case

By Paul Meller, IDG News Service MARCH 12, 2002

BRUSSELS -- In a bid to settle its European antitrust case, Microsoft Corp. said today that it will submit an offer to the European Commission to grant rivals access to two of the technical standards needed to make full use of its Windows operating systems.

John Frank, senior European counsel for Microsoft in Europe, said that by releasing Microsoft's technical information on an encryption system called Kerberos and an Internet standard known as the Common



Internet File System, the software company hoped to address the concerns of the European Commission's competition officials.

"We will be explaining how these steps we are taking are responsive to the concerns raised in the commission's statement of objections," Frank said.

The commission, the executive body of the European Union, has accused Microsoft of abusing its dominance in operating system software to dominate other markets, such as the market for server software. It also alleges that Microsoft has used its operating system muscle to dominate the market for audio- and video-playing software with its Media Player product (see story).

Frank said he hopes that what Microsoft offered to the U.S. Department of Justice will meet this concern of the European Commission.

In the U.S., Microsoft offered to disclose technical information that would allow PC manufacturers to set competitors' software as the default media player. "I don't know if it is enough for the Commission, but it is direct on the point," Frank said.

Intense negotiations between the commission and Microsoft are expected in the coming weeks. Commission spokeswoman Amelia Torres said the group is waiting for proposals from the company.

Microsoft will be submitting separate responses during the coming weeks, Frank said. He declined to estimate when the antitrust case will be over.

"Timing is entirely up to the commission," he said. "I imagine they will be watching events in the U.S. I hope it is over by the end of the year, but I can imagine circumstances where it is not."

Related links:

- Complete Computerworld coverage of Microsoft's legal battles
- What do you think about the antitrust case? Post your opinion in our online discussion forum.
- Judge Thomas Penfield Jackson's ruling, U.S. Government Printing Office Web site
- . U.S. Court of Appeals proceedings in the antitrust case
- · Microsoft statements and legal documents in the case
- · Department of Justice legal documents in the case

MICROSOFT LEGAL ISSUES

Recent Headlines

- Massachusetts investigating Microsoft antitrust settlement
- News Briefs
- Microsoft Freed From Carrying Sun's Java
- Update: U.S. Appeals Court sides with Microsoft on Java

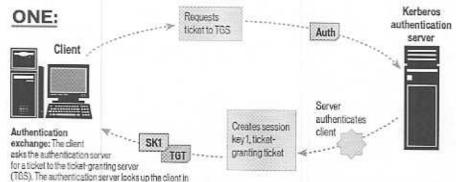
Resources

- What do you think about the antitrust case? Post your opinion in our online discussion forum.
- U.S. District Court documents in the antitrust case
- Microsoft statements and legal documents
- Department of Justice legal documents

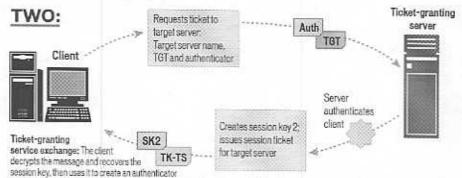
Additional Coverage

■ View our Microsoft Legal Issues special coverage page Computerworld coverage of Microsoft's legal battles.
■ "Microsoft Legal Issues" RSS feed
XML news feed F.A.Q.

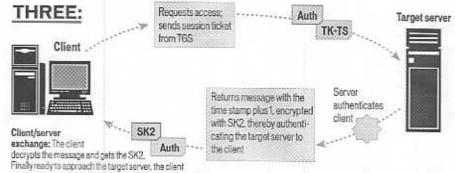
Sharing a Secret: How Kerberos Works



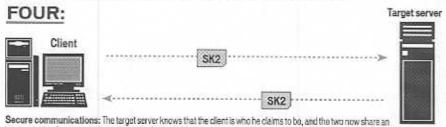
its database, then generates a session key (SK1) for use between the client and the TGS. Kerberos encrypts the SK1 using the client's secret key. The authentication server also uses the TGS's secret key (known only to the authentication server and the TGS) to create and send the user a ticket-granting ticket (TGT).



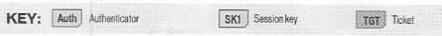
containing the user's name, IP address and a time stamp. The client sends this authenticator, along with the TGT, to the TGS, requesting access to the target server. The TGS decrypts the TGT, then uses the SK1 inside the TGT to decrypt the authenticator, it ventiles information in the authenticator, the ticket, the client's network address and the time stamp. If everything matches, it lets the request proceed. Then the TGS creates a new session key (SK2) for the client and target server to use, encrypts it using SK1 and sends it to the client. The TGS also sends a new ticket containing the client's name, network address, a time stamp and an expiration time for the ticket – all encrypted with the target server's secret key – and the name of the server.



creates a new authenticator encrypted with SK2. The client sends the session ticket (already encrypted with the target server's secret key) and the encrypted authenticator. Because the authenticator contains plaintest encrypted with SK2, it proves that the client knows the key. The encrypted time stamp prevents an eavesdropper from recording both the ticket and authenticator and replaying them later. The target server decrypts and checks the ticket, authenticator, client address and time stamp. For applications that require two-way authentication, the target server returns a message consisting of the time stamp plus 1, encrypted with SK2. This proves to the client that the server actually knew its own secret key and thus could decrypt the ticket and the authenticator.



Secure communications: The larget server knows that the client is who he claims to be, and the two now share an encryption key for secure communications. Because only the client and larget server share this key, they can assume that a recent message encrypted in that key originated with the other party.



Editor's note: This description was adapted and considerably simplified from Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd Edition, by Bruce Schneier (Wiley, 1995).



The Gates of Hades

By Joe Barr Originally published

Printed from LinuxWorld.com

http://www.linuxworld.com/lw-2000-04/lw-04-vcontrol 3.html

Summary

Microsoft's skill at using its Windows monopoly to kill competitors is legendary, and now Kerberos seems to be the next target. This week Joe Barr takes off on an odyssey to uncover Redmond's plan. (1,600 words)

an you imagine Bill Gates as Hercules?
With all due respect to the founder and former CEO of Microsoft, he looks a bit wimpy to play the role of one of the most powerful heroes of Greek mythology. But looks can be deceptive: Gates probably wields more clout than any other businessman on the planet.

With the recent launch of Windows 2000 and its proprietary version of Kerberos, Gates and company seem to be embarking on a journey that is eerily similar to the last of the 12 labors of Hercules: the capture of Kerberos, the three-headed hound who guarded the gates of Hades. Today's Kerberos is different, however.

In May of 1983, MIT established the Athena Project to help explore new uses for its

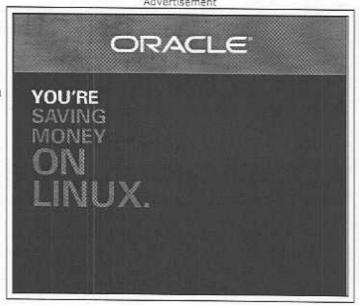
computing facilities. The Athena Project, in turn, gave birth to both the X Window system that is so widely used by almost every flavor of Unix these days, including Linux, and to Kerberos, the computer network authentication system given the name of the aforementioned hound.

What exactly is Kerberos? According to the FAQ (see the <u>Resources</u> section below), "Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography." Kerberos allows you to log on to other computers on a network without fear that your password will be sniffed and compromised.

Over the years, Kerberos has matured and become an open standard. Indeed, the Kerberos standard today is in the hands of the Common Authentication Technology working group of the Internet Engineering Task Force (IETF). But there is a dark cloud on the Kerberos open standard horizon these days. It's been there since the launch of Windows 2000 in February.

Windows 2000 is Microsoft's first implementation of Kerberos. Microsoft has struggled in the past to convince the enterprise market segment that Windows NT is ready to take its place alongside Unix. Certainly Microsoft's reputation for poor security implementation has not helped it in that cause. By embracing the de facto Unix standard for secure authentication, it hopes to become more acceptable in that regard.

All of which is well and good, except for one thing. Microsoft didn't just embrace Kerberos, it has extended it in the classic manner. Microsoft's implementation of Kerberos includes unpublished changes



to the ticket, a security token that allows a client to identify itself to other resources on the network. By taking a public standard private, Microsoft appears to be making another effort to force the adoption of its flagship product with the weight of its market power.

How does that undocumented change to the ticket affect an existing Unix-based Kerberos environment? To find out I spoke with two men who certainly should know: Jeremy Allison, whose work on Samba has brought him into close personal contact with Windows 2000 and its peculiarities, and Ted Ts'o, who worked on the Kerberos development team at MIT from 1990 through 1999.

Speaking of Windows 2000 as it affects Samba, Jeremy (who subscribes to the rule that one should "never ascribe to maliciousness that which can be adequately explained by incompetence") told me a lot of little things broke with the Samba and Windows interface with the release of Windows 2000 but nothing major.

As one example, Allison said, "These are just new peculiarities in Windows 2000 clients, so that it does things like, if you use an SMB client to request a list of shares, we are capable of processing return data of any size, so we request the maximum, which is 64 KB. Now if you request that from a Windows 2000 box, it claims that it doesn't have enough memory to satisfy that. So you have to set it to request 64 KB minus 14 bytes."

But when speaking of Windows 2000 and Kerberos, Allison's view is much different. He told me that the undocumented change prevents Windows 2000 clients from working with existing Unix Kerberos infrastructures. The fix is to install Windows 2000 Kerberos servers.

You can make Windows 2000 and Unix Kerberos servers work together through the tedious -- and less secure -- workaround of storing all client data on both domain controllers and keeping them in synch with one another. But as Allison notes, "it's a terrible pain to try to keep all the Kerberos passwords in synchronization. If you want to have the Unix-based infrastructure, wouldn't it just be easier to move everything over to Windows 2000? Because hey, the Unix servers and clients will work with it anyway since they don't need the extra embraced and extended field."

Ts'o, who left MIT last year to work for VA Linux, has an even darker view of Microsoft's intentions. I asked Ts'o if he believed the Windows 2000 Kerberos implementation was a deliberate strategy. "That is obviously what is going on," Ted said. "If you look at the pattern of behavior, Microsoft has traditionally done this, which is, quote-unquote, 'embrace, extend, and then extinguish.' In the case of telnet authentication, they added their Microsoft authentication, and they've refused to release the specs for how they extended the protocol."

When I asked about Microsoft's earlier promise to document their Kerberos extension, Ts'o provided a bit of history on the issue. "They promised to do so at a public conference where there were a lot of people from the academic sites, where Kerberos has been most popularly used," he said. "It was probably late 1998 or early '98 even, when they made this pledge."

But today, Ts'o said, Microsoft takes another position. "A lot of people from the various educational sites heard that promise," he said. "Now there is this question which is whether or not the person who made that promise was speaking on behalf of Microsoft or not. It's basically turned into a 'we disavow any knowledge of your actions' sort of thing. Microsoft reneged on that promise, or you can say that employee was not authorized to make that promise, choose whichever interpretation you like."

But the fact is that Windows 2000 and its Kerberos implementation have now been on the market for

about two months, and the extension remains a proprietary secret. On April 4, I sent a query about Windows 2000 and Kerberos for Microsoft to Microsoft employee John Brezak, who participates regularly in the comp.protocols.kerberos newsgroup. He has yet to answer any of my questions, and I'm not holding my breath.

Ts'o painted a very monopolistic picture as he explained why he believes Microsoft has attacked the Kerberos open standard in this manner. "I can think of a number of reasons why they want to do that," he said. "The most obvious one is that they want to force everyone to use the PDC, primary domain controller, to be a Windows 2000 server... It's not just Kerberos -- it's also Active Directory and LDAP with all of their extensions, proprietary doo-dahs added on to it. That ties in with the Windows DNA stuff, where they are actually trying to leverage the Windows 2000 infrastructure into things such as Windows CE boxes... it is very clear that the way they are doing things is such that it pretty much guarantees that nobody else can compete because they are not letting anyone else know what the protocols are."

Will Microsoft's assault on open standards continue in the face of its current legal woes? My guess is no. The court-enforced remedies will eventually prohibit that type of predatory behavior. In the meantime, IDC recently reported that Linux's share of the server market is up 166 percent in the 12 months ending on the fourth quarter of last year. That fact clearly shows that Microsoft's questionable business practices have not yet slowed the huge shift away from its closed, proprietary servers to free and open source software solutions.

I also think Gates and company would be wise to study a little more Greek mythology before continuing their efforts to turn an open source standard into a proprietary pit bull. After all, Hercules alone among the Greek heroes went insane and killed his children. One scholar suggests that the reason for Hercules' downfall was his inability to compromise with his own heroic ego.

About the author

Joe Barr is a contributing editor at LinuxWorld and a recovering programmer. In addition to writing for LinuxWorld and The Dweebspeak Primer, he is currently working with Nicholas Petreley on a Linux documentation project called <u>The Essential Linux Open Book</u>. Visit Joe's <u>Linux Desktop discussion</u> in the new Linux Forum, hosted on ITworld.com.

Resources

Kerberos History:

http://staff.washington.edu/rlmorgan/talk/kerberos.1999.06/history.html

What is Kerberos? :

http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html#whatis

· The MIT Kerberos Team:

http://web.mit.edu/kerberos/www/krbdev.html

· Overview of the IETF:

http://www.ietf.org/overview.html

"Windows 2000 Complicates Interoperability for Samba," Stephen Swoyer (InformationWeek, April 3, 2000):

http://www.informationweek.com/780/novel2.htm

Samba's homepage:

http://www.samba.org

"IDC Declares Linux is Red Hot in the Server Market," from Idc.com, 2000:

http://www.idc.com/Data/Enterprise/content/ES041000PR.htm

 "Soul and Body," a chapter from Daimonic Reality by Patrick Harpur: http://www.deoxy.org/soulbody.htm



NetworkWorldFusion

This story appeared on Network World Fusion at http://www.nwfusion.com/news/2000/0424kerberos.html

Observers skeptical of Win 2000 Kerberos plan

Critics see issues with licensing, interoperability.

By John Fontana Network World, 04/24/00

In an attempt to answer interoperability questions about its implementation of Kerberos security in Windows 2000, Microsoft is finally preparing to reveal a key proprietary data format it has been guarding for nearly two years.

But while IT executives and standards watchers have hoped that Microsoft would publish the data format, they are now concerned about a possible Microsoft plan to license the technology instead of making it freely available. They say that action would continue to needlessly tie Kerberos users to Win 2000.

Kerberos is an Internet Engineering Task Force standard authentication and authorization mechanism. Ideally, a standards-based implementation of Kerberos allows for network or Internetwide authentication and authorization regardless of the network operating system.

But Microsoft's implementation of Kerberos uses proprietary data, called a Privilege Access Certificate (PAC), in its Kerberos "tickets." The result is that tickets generated by third-party Kerberos servers, or Key Distribution Centers (KDC), are not valid to access Windows resources, such as files, applications or network devices, even though the KDCs are built around the same Kerberos Version 5 standard.

Microsoft has been saying for more than two years that it would publish PAC data as a way to foster interoperability.

Microsoft followed the Kerberos Version 5 specification but used the PAC in the specification's "authdata field" on the Kerberos ticket to insert Windows Secure ID information that bounds tickets to Windows Access Control Lists.

The Open Group, which develops DCE Kerberos, and the Massachusetts Institute of Technology, which develops a free KDC, also use the auth-data field to provide user ID but freely publish the data format.

Customers want Microsoft to address the restriction.

"Yes, I would like to see this information published, but whether it would help us with interoperability, I

really don't know yet," says Al Williams, director of distributed systems services at Pennsylvania State University's Center for Academic Computing. He has more than 200,000 Kerberos user IDs on a Unix-based KDC and is rolling out Win 2000. Williams says he does not want licensing restrictions and he would not consider Microsoft's Kerberos "standards-based" if licenses are required.

"An open model tends to encourage cooperative partnerships. We feel that type of arrangement is better for all involved," Williams says.

Microsoft officials would not comment on their plans for publishing the PAC data.

Regardless, some say requiring PAC licenses is a way to keep Kerberos users tied to Microsoft.

"We are happy they are living up to their promise of disclosure [of the PAC]," says Paul Hill, a senior programmer analyst at MIT and a member of Kerberos Version 5 development team. "But we are not really happy that they want everyone to license the technology."

MIT's version of Kerberos is freely available, and Hill says MIT won't license the PAC for its server. "How would we pay for it? Our server is free. Putting PAC support in our server just won't happen," he says.

Microsoft, according to sources, hopes developers use the PAC in their applications, therefore tying them into the Win 2000 KDC. That would force non-Windows KDCs to have a trust relationship with Win 2000 KDCs in order to access those applications.

Microsoft could also allow KDC vendors to license and "clone" the PAC on their KDC without running a Win 2000 KDC, but it is not clear if that will be permitted. That would let users bypass Win 2000 and rely on a Unix KDC. But users running Kerberos and Windows applications - such as SQL, Exchange or Internet Information Server - would still have to pay Microsoft for either Win 2000 or for the PAC data format to support access to those resources from a non-Microsoft KDC.

"Microsoft is using its dominance in the application market to help create a monopoly in the server market," Hill says. He's happy Microsoft is using Kerberos because it improves security across the Internet, but "for anyone who runs a competing KDC, Microsoft has usurped the standard and is destroying interoperability."

Analysts say Microsoft is carrying out its unique view of integration.

"This Kerberos tactic is more subtle than usual, but this is the way they promote one technology with another," says Michael Gartenberg, an analyst with the Gartner Group.

Related Links

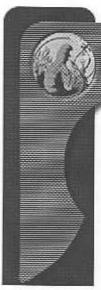
Newsletter: Kerberos and Windows 2000 Network World, 03/13/00.

Microsoft, others target Kerberos interoperability Network World, 02/07/00.

Interoperability issues bite Win 2000 Kerberos scheme Network World, 09/13/99.

Kerberos cryptography secures NT 5 communications Network World, 7/20/98.

All contents copyright 1995-2002 Network World, Inc. http://www.nwfusion.com



it-analysis.com

Home | Analysis | Archive | Research | Events | Register



Famous Slights - "The one function that TV news performs very well is that when there is no news we give it to you with the same emphasis as if it were." - David Brinkley New Quote

READER COMMENTS

Is Kerberos about to get resurgence?



With the arrival of Windows Server 2003 we might be forgiven if we think that Kerberos is on its way out. Talk to Microsoft people and you might find an unusual ambivalence to Kerberos. It is somewhat refreshing therefore to find a new Kerberos product on the market.

Reader Comment / Feedback

Ambivalence may not be how Microsoft looks at Kerberos. One thing certain is that Kerberos is definitely not on the way out in Microsoft Windows 2003 and XP Professional. Microsoft has definitely pushed PKI harder on the basis of the new and exciting PKI components in Windows 2003 as against, the counterparts in Windows 2000.

A quick reading into Microsoft.com

(http://www.microsoft.com/windowsxp/pro/techinfo/planning/pkiwinxp/default.a sp) will tell us just the contrary that the Microsoft - Kerberos affair is far from over - not if Kerberos is among the top 10 reasons why one should migrate to Windows 2003.

(http://www.microsoft.com/windowsserver2003/evaluation/whyupgrade/top10 nt.mspx) .

Quoting from Microsoft.com

"Windows XP Professional and Windows Server 2003 expand and enhance the management and performance features of the Windows 2000 security infrastructure. These improvements include Increased Kerberos performance"

"Windows Server 2003 lets you securely extend your network to employees, partners, and customers by integrating Virtual Private Network (VPN) services, standards-based authentication, and encryption technologies. Flexible authentication options include: Kerberos"

Venkat Krishna

- John, I would like to comment on a few points in your article and make the CyberSafe product positioning clearer:
 - The WebAccess product is designed for use on Intranet or Extranet environments where users are already authenticating themselves using Kerberos when they log into the Microsoft Active Directory domain. The credentials

obtained during this login process are then used to identify the user to Web applications on the Intranet or Extranet. The use of Kerberos in this environment allows exploitation of credential delegation, mutual authentication and network replay attack detection for added benefit - these would not be possible if just using PKI technology in a Web environment.

- 2. The use of PKI in a Web environment is completely complimentary and NOT COMPETITIVE with the solutions offered by the WebAccess product. When using PKI in a Web environment the users private key can be used to sign forms/objects etc. which Kerberos is not capable of doing, and Kerberos is capable of solving other security needs in a Web environment which PKI cannot the conclusion is that both Kerberos and PKI are useful for Web application security.
- 3. Microsoft introduced Kerberos authentication into IE 6.0 and IIS 5 when Win2k was launched 3 years ago - the CyberSafe WebAccess product simply takes this same approach into a heterogeneous environment so that non-MS Web servers, applications and operating systems can be used. If a company has a mixture of IIS and Apache in their network they can use the same user credentials from the workstation login for both Web server environments.

Thanks, Tim. Tim Alsop

The messages above were all contributed by IT-Analysis.com readers. Whilst Bloor Research takes care to remove any posts deemed inappropriate, we can take no responsibility for the content above.

POST A COMMENT

Comment	
Name/Alias	(Mar)
Email (Not displayed)	
POST COMMENT	

Brian Livingston



HOME/ SITEMAP SUBJECT INDEXES App Development Broadband Business Intell. Business News Business Strategies Careers & Mgmt Collab. Software Content Mgmt CRM

Database E-Business End-User Apps

End-User Hardware Enterprise Apps Ethics Government

Licensing Middleware

Mobile Computing Networking Online Community

Operating Systems Processors Security Servers

Storage Telecomm.

Web Services

Web Technologies Wireless XSPs

NEWS CTO ZONE TEST CENTER FEATURES COMMUNITY OPINIONS RESEARCH EVENT

WEBCASTS ABOUT InfoWorld

* ABOUT US

About InfoWorld Services Advertise Contact us Employment

Learn to secure your PCs from new

EARCH:	News	GO	Google
Home // Article			
NEWS			

Is Microsoft's change in Kerberos security a form of 'embrace, extend, extinguish'?

LAST WEEK, I mentioned in passing that Microsoft had included in Windows 2000 a nonstandard version of the Kerberos security protocol. This subject bears a little more explanation.

The Kerberos standard is named for the mythological three-headed dog that guards the gates of Hades. It's used to authenticate users logging on to a server. Unlike NT LAN Manager (NTLM) authentication -- the LAN Manager-style authentication in Windows NT 4.0 -- Kerberos uses a more efficient "single sign-on" method to maintain security between users and servers on a variety of operating systems. Kerberos was originally developed at the Massachusetts Institute of Technology (MIT) in the early 1990s. The Internet Engineering Task Force (IETF) then adopted it as a networking standard (see www.ietf.org/rfc/rfc1510.txt for details).

Microsoft released Win2000 Feb. 17, with Kerberos replacing the weaker NTLM security protocol. But outside observers noted angrily that PCs using Win2000 Professional couldn't exchange authorization information via standard Kerberos with Unix servers and others. This keeps the servers from providing access control in a domain -- unless the servers are Win2000.

Critics said Microsoft's change to the standard was part of an "embrace, extend, and extinguish" strategy. "They want to force everyone to use ... a Win2000 server," said Ted Ts'o, a former member of MIT's Kerberos development team, in the April 2000 Linux World (see www.linuxworld.com/linuxworld/lw-2000-04/f lw-04-vcontrol 3.html).

During much of the Win2000 beta test, networking pros demanded that Microsoft reveal the secrets of its modifications to Kerberos. Microsoft developers said at various times that the company would do so.

On April 28, after my last column had been written, Microsoft posted on its Web site a document that explains the changes (see ▼ WHITE PAPERS www.microsoft.com/technet/security/kerberos/default.asp). Microsoft had made use of an Authorization Data field that IETF had left undefined for future use.

and unknown hacker attacks.

Free IDC White Paper - Discover Secure File Sharing for the Enterpriseattacks. The posting only raised more suspicions. To run the self-extracting file that installs the document, you must click OK to accept a nondisclosure agreement. It states that the information in the document is a "trade secret of Microsoft" and you aren't licensed to use future versions or extensions of the standard.

Of course, you can bypass the agreement by opening the self-extracting file in WinZip before viewing it. The federal law's definition of "trade secret" stipulates that "the owner thereof has taken reasonable measures to keep such information secret." So it's unlikely that Microsoft could legally enforce nondisclosure.

The mere threat of legal action, of course, is enough to chill most competitive development. Jeremy Allison, a member of the open-source Samba project, said in an Internet newsgroup, "This, of course, is a very clever way to pretend to distribute the spec, whilst making it completely impossible to implement in open-source Kerberos servers" (see linuxtoday.com/stories/21066.html).

I sent an e-mail message to Microsoft asking about the "trade secret." A spokesman said an official response was held up in the aftermath of the "I Love You" worm that affected Microsoft's e-mail system.

Meanwhile, Bryan Muehlberger, principal at DirectPoint Information Group, a St. Louis-based Microsoft Certified Solution Provider, offered a sympathetic view.

"Microsoft has made use of an available field, but not in a way that it was intended to be used -- and, of course, didn't document or mention this change anywhere," Muehlberger said. "In Microsoft's defense, they have to use the field this way. Basically, Microsoft has included in this field the SIDs [security identifiers] that specify a user's role/access to a particular resource. Since all resources in a Win2000 environment are protected by access control lists, if Microsoft did not include the SIDs in this field, then the resource would have to contact the Domain Controller for this information -- just like it does with NT LAN Manager authentication -- which hurts in terms of optimization."

What's your opinion? Send me your thoughts, using "Kerberos" as the subject.

Brian Livingston 's latest book is Windows 2000 Secrets (IDG Books). Send comments to brian_livingston@infoworld.com . He regrets that he cannot answer individual questions.

RELATED SUBJECTS

▶ Operating Systems

MORE >

SUBSCRIBE TO: ▶ E-mail Newsletters ▶ InfoWorld

Mobile > InfoWorld Magazine

Home // Article



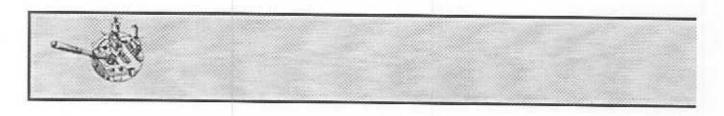






ADVERTISEMENT

SPONSORED LINKS



Kerberos: Computer Security's Hellhound

By Andrew Conry-Murray 07/05/2001 9:50 AM EST URL: http://www.networkmagazine.com/shared/article/showArticle.jhtml? articleId=8703147

Guard dogs are great if you're protecting a house or a military base. But when it comes to securing nodes on a computer network, guard dogs don't scale. Just try installing German shepherds on your users' desktops and you'll see what I mean.

However, there is one dog you can install for computer security: Kerberos. Kerberos is an authentication protocol that lets clients and servers reliably verify each other's identity before establishing a network connection. Developed at MIT in the late 1980s, Kerberos takes its name from the three-headed hound in Greek mythology that guards the entrance to Hades. But instead of guarding the underworld, today's Kerberos brings a measure of security to a distributed computer environment, where one computer can access the resources of any other machine on a network.

Paul Hill, information systems senior programmer at MIT and a member of the Kerberos development team since 1992, outlines the benefits of the Kerberos system. First, it has been subjected to public review for over a decade. Second, version 5 of the protocol-the most current version-was developed within the IETF standards process. Finally, Kerberos provides for secure authentication and message integrity, as well as data confidentiality and mutual authentication between a client and a server.

Kerberos assumes that packets traveling on a network may be subject to viewing, interception, and tampering. Thus, Kerberos combines passwords and symmetric key encryption to authenticate users and protect communications. The protocol supports DES and TripleDES encryption.

MIT makes the source code freely available to anyone who wants it, but commercial versions are also on the market. With its university origins and Unix-based development, Kerberos has traditionally been used in colleges and universities, though it's also a favorite of financial institutions. With Kerberos' inclusion in Microsoft's Windows 2000 operating system, the authentication protocol now has the potential to reach a much wider user and developer audience.

As might be expected, the adoption of an open source protocol by Microsoft

has been greeted with both pleasure and dismay. While Microsoft's use of the protocol has certainly raised Kerberos' profile, Microsoft has also tinkered with it by adding proprietary functions, creating the potential for interoperability issues in environments that run both Unix and Microsoft Kerberos.

This article focuses on the basic workings of Kerberos, examines the ramifications of the Microsoft implementation, and discusses the future of the Kerberos protocol.

Kerberos Basics

Like Kerberos the dog, Kerberos the protocol has three heads: two principals and one trusted third party. The principals are two devices, usually a client and a server, that wish to communicate with each other. Each principal has its own unique long-term password (for instance, the password that a human user types in at login each morning). The trusted third party, the Key Distribution Center (KDC), mediates by providing a secret for two principals to share between themselves. The KDC also knows the password of each and every principal that it mediates for. It keeps those passwords in an encrypted database.

Kerberos uses secret key cryptography, otherwise known as symmetric key cryptography, to function. In secret key cryptography, a plaintext message can be converted into ciphertext (that is, unintelligible data) and then converted back to plaintext using one key. Thus, two principals will share a secret key to encrypt and decrypt their communications.

Note that secret key cryptography is different from asymmetric key cryptography, or public key cryptography, in which a principal has both a public and a private key. The private key is never shared.

A Kerberos transaction consists of session keys and tickets. A session key is a secret key prepared specifically for two principals to share authentication data and provide message integrity and confidentiality. A ticket contains important information about the transaction and gives the ticket requester access to another machine. A client has to get a session key and a ticket for each machine it wants access to.

The information in a ticket includes a timestamp that states when the ticket was created and an expiration time for the ticket. The principals use the timestamp as an authentication mechanism, so it's important to synchronize the principals' clocks as closely as possible.

The expiration time determines how long a ticket is valid. This is a security measure to limit the damage an intruder might cause by somehow "hijacking" a ticket. A common ticket lifetime is a standard work-day, but administrators can adjust the expiration to be as short or long as they want, depending on the organization's security stance. Keep in mind that shorter expiration times may generate more traffic as principals continuously reauthenticate (and may

annoy end users, who must repeatedly retype their passwords).

Depending on the size of your network, you can divide principals among multiple KDCs by creating "realms." A realm consists of all the principals that have a direct trust relationship with a single KDC. Principals in one realm can communicate with principals in another realm through a process known as cross-realm authentication.

Tickets Please

This section details a basic Kerberos transaction between two principals in a Kerberos environment. For the sake of argument, let's say Alice is a user on a client workstation and Bob is a server that Alice wants access to.

In a Kerberos environment, the authentication process begins at login. Alice enters her user name and password into her client workstation. The workstation sends Alice's user name to the KDC. The KDC contains a master database of unique, long-term keys for every principal in its realm. The KDC looks up Alice's master key (KA), which is based on Alice's password. The KDC then creates two items: a session key (SA) to share with Alice, and a Ticket-Granting Ticket (TGT). The TGT includes a second copy of the session key (SA), Alice's user name, and an expiration time. The KDC encrypts this ticket using its own master key (KKDC), which only the KDC knows.

The KDC then encrypts all of this information with Alice's master key (KA) and sends it to her workstation. The workstation receives this information, which basically looks like a jumble of random bits, and runs Alice's password through a one-way hashing function, converting her password into her master key (KA). Using Alice's master key, the workstation decrypts the package. The workstation now has a session key that it shares with the KDC and a TGT. The workstation can "forget" Alice's master key because it will simply use the session key (SA) and TGT for subsequent communication with the KDC.

Let's say Alice attempts to access Bob (see <u>figure</u>). Instead of contacting Bob directly, Alice's workstation contacts the KDC. The contact consists of the TGT, a request to access Bob, and a piece of data called an authenticator. The authenticator is a timestamp. This authenticator is encrypted using the session key that Alice shares with the KDC (SA).

The KDC decrypts the TGT using its own master key (KKDC). As you'll recall, the TGT contains Alice's user name and a copy of the shared session key (SA). The KDC uses this shared session key (SA) to decrypt the authenticator. The KDC can confirm that this request actually comes from Alice because only Alice can use the shared session key (SA).

Next, the KDC creates a pair of tickets, one for Alice and one for Bob. Each ticket contains essential information, including the name of the principal requesting the service, the recipient of the request, a timestamp that declares

when the ticket was created, and a time duration that says how long the tickets are valid. Both tickets also contain a new key (KAB) that will be shared between Alice and Bob.

The KDC takes Bob's ticket and encrypts it using Bob's master key (KB). Then the KDC nests Bob's ticket inside Alice's ticket, which also contains the new key (KAB), as well as the other data. The KDC encrypts the whole thing using the session key that it shares with Alice (SA). The KDC then sends it all to Alice.

What happens next? When Alice receives the ticket, she decrypts it using the session key (SA). This reveals the new session key (KAB) and the ticket for Bob. Alice can't read Bob's ticket. Alice then encrypts the authenticator (the timestamp) using the new key (KAB) and sends the authenticator and Bob's ticket to Bob. On receiving these two items, Bob first decrypts his own ticket using his master key (KB). This permits access to the new session key (KAB), which can then decrypt the authenticator from Alice.

Now both Alice and Bob have the new key (KAB). Bob can be sure that Alice is who Alice claims to be because Alice used the key (KAB) to encrypt the authenticator. If it's necessary for Bob to respond to Alice, Bob will use the new key (KAB). Alice will know that Bob is who he claims to be because Bob had to use his master key (KB) to get the new key (KAB).

Alice can authenticate herself to other principals in a similar fashion. For each communication request, the KDC will create a unique session key for the principals involved.

If your brain hasn't melted yet, congratulations. In any case, keep in mind that this authentication function is invisible to end users, and happens in seconds rather than in the minutes it takes to read a description of the process.

Embrace, Extend, and Annoy

Kerberos version 5 has replaced Micro- soft's NT LAN Manager (NTLM) as the primary network authentication method for Windows 2000. (NTLM is also included for backward compatibility.) Microsoft cites several benefits of Kerberos as compared to NTLM, including more efficient authentication to servers, mutual authentication, simplified trust management, and interoperability.

"From our perspective, it was a good industry protocol to support and was one of the things that would be good to add to the overall platform," says Jackson Shaw, product manager for the Windows 2000 Server.

Kerberos promoters outside of the Microsoft camp are cautiously optimistic about the protocol's inclusion. "I think it was very good for Kerberos," says Dr. Clifford Neuman. Dr. Neuman was the principal designer of Kerberos at MIT, and is now chief scientist at CyberSafe, a security vendor that sells a commercial version of Kerberos. He says Microsoft's market dominance

"increases the desire of vendors to have Kerberos authentication integrated with their particular applications and utilities."

MIT's Hill also seems pleased (with a few reservations) about the implementation. "I think everyone in the industry has learned to be cautious when dealing with Microsoft, and people are very wary about any extensions that Microsoft introduces. But overall I think their adoption of Kerberos is positive. Any time you have a large vendor deciding to use a standard protocol, it's a good thing."

However, while Microsoft's adoption of the protocol is a feather in the cap for Kerberos, Microsoft has frustrated members of the Unix Kerberos community by adding proprietary information to this open source standard.

"Microsoft couldn't just put Kerberos in, they had to 'embrace and extend' it in order to add some extra data in a way that some people feel violated the spirit, but not the letter, of the specification," says Mark Van Heyningen, Internet security architect and Kerberos aficionado at security vendor Aventail.

The problem revolves around an optional data field in Kerberos version 5 called the authorization data field. Microsoft has added a Privilege Access Certificate (PAC) to the data field. By using the PAC in this field, Windows 2000 adds authorization capabilities to Kerberos that will manage a user's privileges based on Windows groups that the user belongs to.

The fact that Microsoft made use of this field isn't an issue. "The use of the PAC field in the standard is left to implementers to implement it in whatever way they want," says Shaw. While this is true, Microsoft has, in the words of Dr. Neuman, attached "onerous restrictions on what can be done" with Microsoft's adaptation of this field.

Those onerous restrictions take the form of a licensing agreement, which basically says that a person can read the specification but not attempt to implement any of the authorization data functions without Microsoft's permission. (See Resources for a link to the license agreement.) Such restrictions are anathema in an open source standard. "I think with respect to open protocols there are still a significant number of people at Microsoft who still don't get it," says Van Heyningen.

So why did Microsoft adopt an open standard and then add proprietary information? The issue revolves around Microsoft's domain controllers. A domain controller provides centralized management of user accounts, machines, and groups. In Windows 2000, the domain controller is also the directory server, the Kerberos KDC, and the origin of group policies that are applied to the domain.

Shaw explains Microsoft's rationalization. "The authorization field is specific to Windows 2000 and how domain controllers interact on the network. The use of this information would allow a non-Microsoft product to simulate a

domain controller. Since the addition of a third-party domain controller could cause unexpected results, we wish to ensure that each company that wishes to implement this type of a product works closely with Microsoft."

Simulating a domain controller is exactly what MIT's Hill would like to do, but can't. "I'm disappointed," he says. "Microsoft's design has an intentional side effect of making sure that no other Kerberos implementer can develop a complete replacement of a Windows 2000 domain controller. This means that MIT couldn't, even within our own campus, create a system where we got all the benefits of a domain controller but actually weren't running a Microsoft domain controller. I'd much rather see people be able to try to emulate the behavior of a domain controller and really compete against Microsoft in their own home market."

There's also the question of interoperability: Will Windows 2000 Kerberos play together with a Unix-based Kerberos implementation?

Microsoft's Shaw is adamant that it will. "You can have a Unix Kerberos system today, and it will and should fully interoperate with Microsoft's Kerberos so a person can perform single sign-on from their Unix system into their Windows system. And if it doesn't, we're very interested in talking to that client because it's something we do want to see work properly."

Hill agrees that basic authentication will still function between Unix Kerberos and the Windows 2000 Kerberos, despite the PAC. "When an application service receives a ticket that has this authorization data in there, and it doesn't know how to use it, it will just ignore it. So that doesn't break anything. It can use the rest of the ticket just fine, as it would any other ticket."

Yet he says there's still the potential for users coming in from a Unix Kerberos realm to be locked out of Windows 2000 services. "If a Microsoft application server receives the ticket without any authorization data, it can authenticate the user, but it can't automatically decide what a user should be allowed to do, like do they have access to a particular resource."

In effect, you can still be authenticated from the Unix Kerberos realm into a Windows 2000 Kerberos realm, but if your ticket lacks the PAC information used by Windows 2000, the system may not know what services you're authorized to use, and thus deny service access.

However, says Hill, there are work- arounds. "If you set up cross-realm properly so that you have both a Unix-hosted KDC and realm working in conjunction with a Microsoft KDC and realm, then it becomes transparent to the user-and everything works just fine." Hill says he finds this fairly easy to do, but can't speak for everyone's experience.

Both Neuman and Hill say that Microsoft has worked closely with their organizations (CyberSafe and MIT, respectively) to ensure interoperability. "I think that the particular people doing development on Kerberos at Microsoft are very reasonable people," says Neuman. "They seem to have a gen-uine

interest in seeing Kerberos as a standard."

Hill concurs. "Microsoft has spent a lot of time and effort converting things to use Kerberos. And they are putting a lot of time and effort into interoperability testing. I feel they're doing a pretty good job on that."

Old Dog, New Tricks

Both MIT and commercial developers are working to improve Kerberos by adding support for the recently released Advanced Encryption Standard (AES), a new, more secure upgrade to the aging DES. Neuman estimates that the MIT release may support AES by the end of summer 2001.

The integration of Kerberos and PKI is also going forward. Hill cites efforts such as PKINIT, PKCROSS, and the University of Michigan's KX.509 project.

In addition, Microsoft's adoption of Kerberos, while raising a few hackles among the open source community, also raises the protocol's profile, and is sure to spur the development of applications that will take advantage of Kerberos authentication.

Most dogs as old as Kerberos would have retired from guard duty years ago, but today the protocol is as robust as ever. Of course, you may not be surprised to find Kerberos still on its toes; after all, it's a hell of a dog.

Andrew Conry-Murray, business editor, can be reached at amurray@cmp.com.

Resources

Kerberos version 5 is discussed in detail in RFC 1510. To read the RFC, go to ftp://ftp. isi.edu/in-notes/rfc1510.txt/.

MIT has a host of information on Kerberos, including FAQs, papers, and security vulnerabilities. Go to http://web.mit.edu/kerberos/www/.

Dr. Clifford Neuman, principal designer of the Kerberos authentication system, has a Web site with many useful links. Go to www.bcneuman.com.

Jim Rome's Web site, "How to Kerberize Your Site", describes how to set up a Kerberos authentication system. It also has links to commercial Kerberos vendors.

Microsoft makes several white papers on Kerberos available. Go to this link and this one.

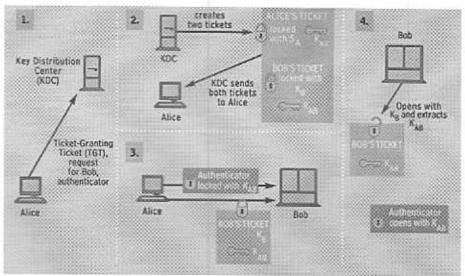
To download the specification on Microsoft's use of the authorization data field, go here and click on the "Kerberos PAC Specification" link at the bottom of the page. You must agree to a license to get access to the

document.

Cryptography and E-Commerce (John Wiley & Sons, 2001), by John C. Graff, is a good introduction to cryptography and authentication techniques, including Kerberos and PKI.

Network Security: Private Communication in a Public World (Prentice Hall, 1995), by Charlie Kaufman, Radia Perlman, and Mike Speciner, has several in-depth chapters on Kerberos.





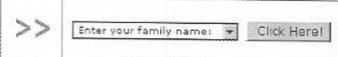
The Authenticator. When Alice wants to authenticate to Bob, she must first contact the Key Distribution Center (KDC). 1) Alice sends her Ticket-Granting Ticket (TGT) and a request to authenticate to Bob to the KDC. 2) The KDC creates two tickets and a new session key (KAB). The KDC nests Bob's ticket inside Alice's ticket. Alice's ticket is encrypted with Alice's secret key (SA), and Bob's ticket with his secret key (KB). Both tickets include the new key (KAB). The KDC returns both tickets to Alice. 3) Alice decrypts her own ticket, revealing the new session key (KAB). Alice then encrypts an authenticator with KAB and sends Bob's ticket and the encrypted authenticator to Bob. 4) Bob decrypts his ticket with KB, revealing the session key (KAB), which he can use to reveal the authenticator from Alice.



Copyright © 1993-2002 The Condé Nast Publications Inc. All rights reserved.

Copyright @ 1994-2002 Wired Digital, Inc. All rights reserved.







Issue 11.06 - June 2003

VIEW essay

Print, this art

Copy Protection Is a Crime

...against humanity. Society is based on bending the rules.

By David Weinberger



Scott Menchin

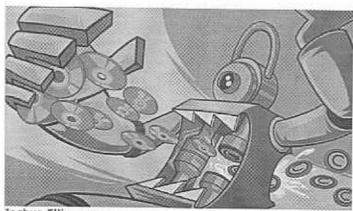
Digital rights management sounds unobjectionable on paper: Consumers purchase certain rights to use creative works and are prevented from violating those rights. Who could balk at that except the pirates? Fair is fair, right? Well, no.

In reality, our legal system usually leaves us wiggle room. What's fair in one case won't be in another - and only human judgment can discern the difference. As we write the rules of use into software and hardware, we are also rewriting the rules we live by as a society, without anyone first bothering to ask if that's OK.

Copy Protec Crime Cyberpunk digital revol is current sr us? Attacking V-Capitalism There's Son Rummy So Much for Principle

The problem starts with the fact that digital content can be copied - perfectly - from one machine another. This has led the recording and movie industries to push for digital rights management sc Buy a one-time right to play the latest hit song or movie, and DRM could prevent you from playing

Of course, to exercise such exquisite control over content, DRM requires deep changes to all parts equation - the hardware, the operating system, and the content itself. Sure enough, some in Conrecently pushed the FCC to add a "broadcast flag" to content which digital hardware would be req honor. DRM is barreling down the pike.



Joshua Ellingson

The usual criticism is that the scheme gives too much power to copyright holders. But there's a diproblem: Perfect enforcement of rules is by its nature unfair. For contrast, consider how imperfect are applied in the real world.

If your lease stipulates that you can't paint without explicit permission from your landlord, you wi nevertheless patch up the scratches made by your yappy little dog on the bottom of the front doo high-priced industry analyst's report warns you on every page against duplicating, you'll still hanc your weekly sales meeting copies of a page with a relevant chart. You'd snicker at the very sugge doing otherwise.

But why? The analyst report is stamped 'DO NOT PHOTOCOPY', and the bit in your lease about no really couldn't be any clearer. We chuckle because we all understand that before the law there's lithe true bedrock of human relationships. Sure, we rely on rules to decide the hard cases, but the the time we cut one another a whole lot of slack. We have to. That's the only way we humans car to share a world. Otherwise, we'd be at one another's throats all the time - or, more exactly, our would be at each other's throats.

Yet we're on the verge of instituting digital rights management. What do computers do best? Obe What do they do worst? Allow latitude. Why? Because computers don't know when to look the oth

We're screwed. Not because we MP3 cowboys and cowgirls will not have to pay for content we've "stealing." No, we're screwed because we're undercutting the basis of our shared intellectual and lives. For us to talk, argue, try out ideas, tear down and build up thoughts, assimilate and approp concepts - heck, just to be together in public - we have to grant all sorts of leeway. That's how id how cultures get built. If any public space needs plenty of light, air, and room to play, it's the ma of ideas.

There are times when rules need to be imposed within that marketplace, whether they're internat against bootleg CDs or the right of someone to sue for libel. But the fact that sometimes we resor shouldn't lead us to think that they are the norm. In fact, leeway is the default and rules are the

Fairness means knowing when to make exceptions. After all, applying rules equally is easy. Any b can do it. It's far harder to know when to bend or even ignore the rules. That requires being sens individual needs, understanding the larger context, balancing competing values, and forgiving transgressions when appropriate.

But in the digital world - the global marketplace of ideas made real - we're on the verge of handir amorphous, context-dependent decisions to hard-coded software incapable of applying the snicke This is a problem, and not one that more and better programming can fix. That would just add mi What we really need is to recognize that the world - online and off - is necessarily imperfect, and

important it stay that way.

David Weinberger (self@evident.com) is the author of Small Pieces Loosely Joined.

Previous Story: Shopping Cart

Next Story: Cyberpunk predicted the digital revolution. What is current sci-fi telling us?

Copyright © 1993-2002 The Condé Nast Publications Inc. All rights reserved.

Copyright © 1994-2002 Wired Digital, Inc. All rights reserved.