MadHat Unspecific
Simple Nomad

SPA: Single Packet Authorization

We needed a protocol that allowed us to tell a server that we are who we say we are, have it work across NAT, use TCP, UDP, or ICMP as the transport mechanism, act as an extra layer of security, and be secure itself. Oh, and do so with a single packet. Sound crazy? It's actually very useful. We've come up with a Single Packet Authorization (SPA). This is a protocol for a remote user to send in a request to a server which I cannot be replayed and which uniquely identifies the user. The proof-of-concept code alone is worthy of a presentation itself, but SPA is so much more. This is not port-knowcking (although SPA can easily replace port-knocking with something much more secure).

MadHat *leads the DC214, Dallas Defcon Group and is a member of NMRC. His paying gig is as the Manager of Vernier Threat Labs. Before working at Vernier, MadHat was one of the core security team members for Yahoo and leat the vulnerability assessment and day-to-day security monitoring for Yahoo world-wide. He has written several open source security tools and has contributed to an upcoming book on NMap being written by Fyodor.*

Simple Nomad *is the founder of the Nomad Mobile Research Centre (NMRC), an international group pf hackers that explore technology. By day he works as a Senior Security Analyst for BindView Corporation. He has spent several years developing and testing various computer systems for security strengths. He has authored numerous papers, developed a number of tools for testing the security and insecurity of computer systems, a frequently-sought lecturer at security conferences, and has been quoted in print and television media outlets regarding computer security and privacy.*

SPA:
Single Packet Authentication

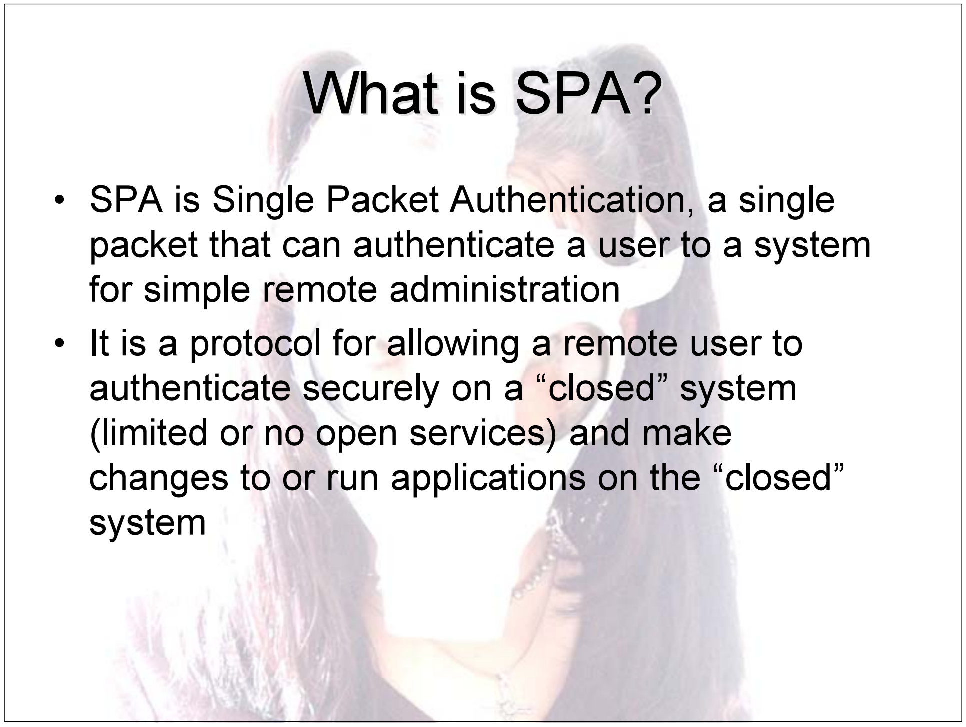
MadHat Unspecific
Simple Nomad
nomad **m**obile **r**esearch **c**entre

Who We Are

- MadHat Unspecific
  - – Hacker, NMRC
  - – Manager, Vernier Threat Labs, Vernier Networks
- Simple Nomad
  - – Hacker, NMRC
  - – Senior Security Analyst, RAZOR Research, BindView Corporation

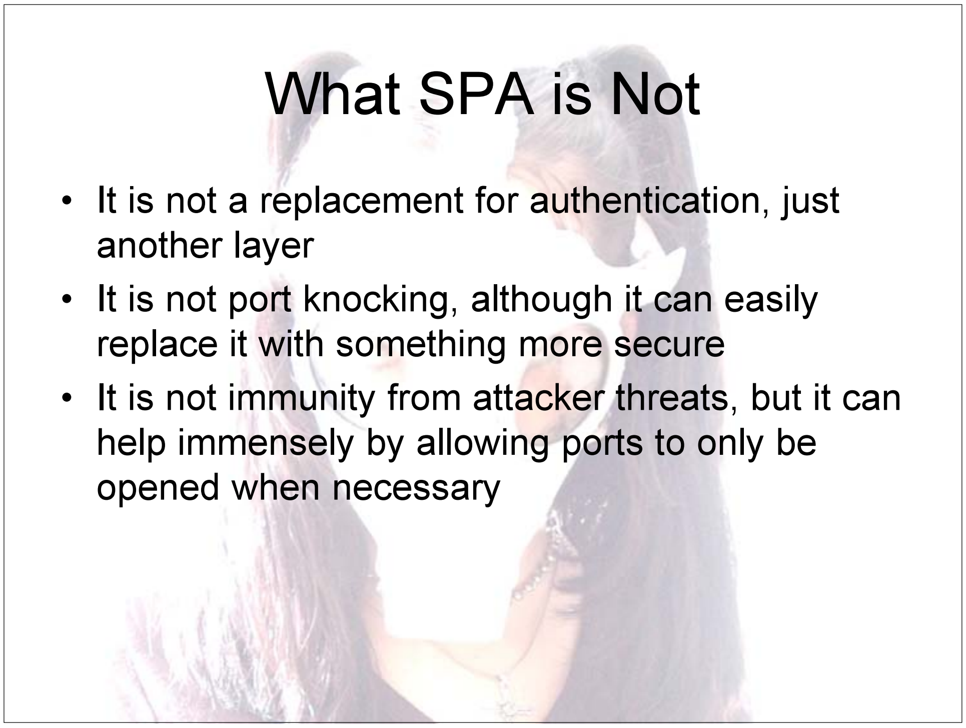
Vernier NETWORKS
BINDVIEW Insight at Work

What Be It?



What is SPA?

- SPA is Single Packet Authentication, a single packet that can authenticate a user to a system for simple remote administration
- It is a protocol for allowing a remote user to authenticate securely on a “closed” system (limited or no open services) and make changes to or run applications on the “closed” system

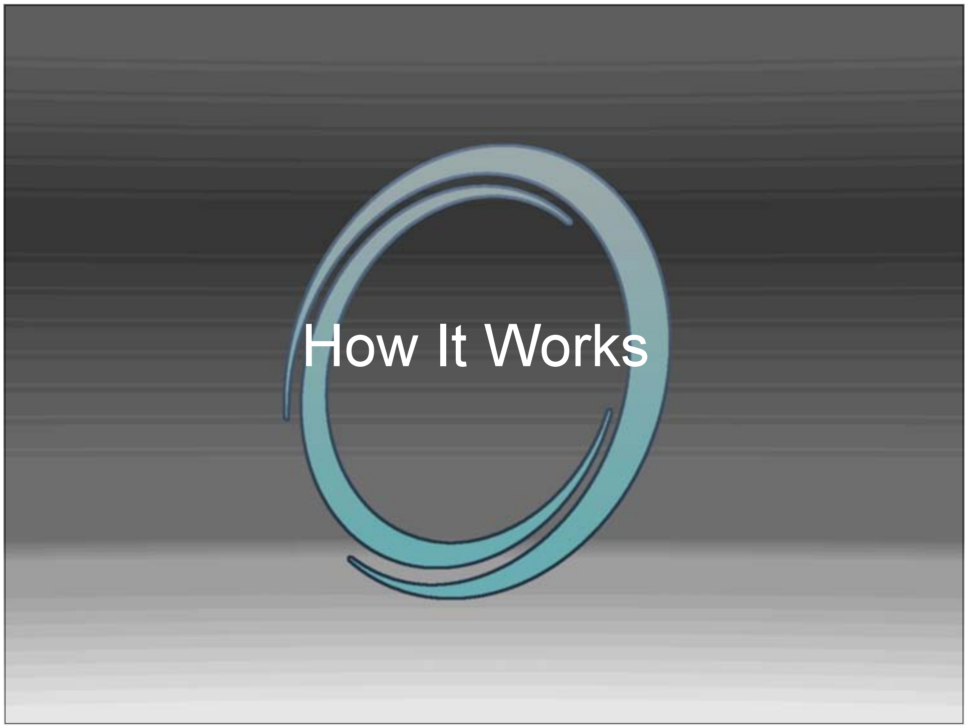


What SPA is Not

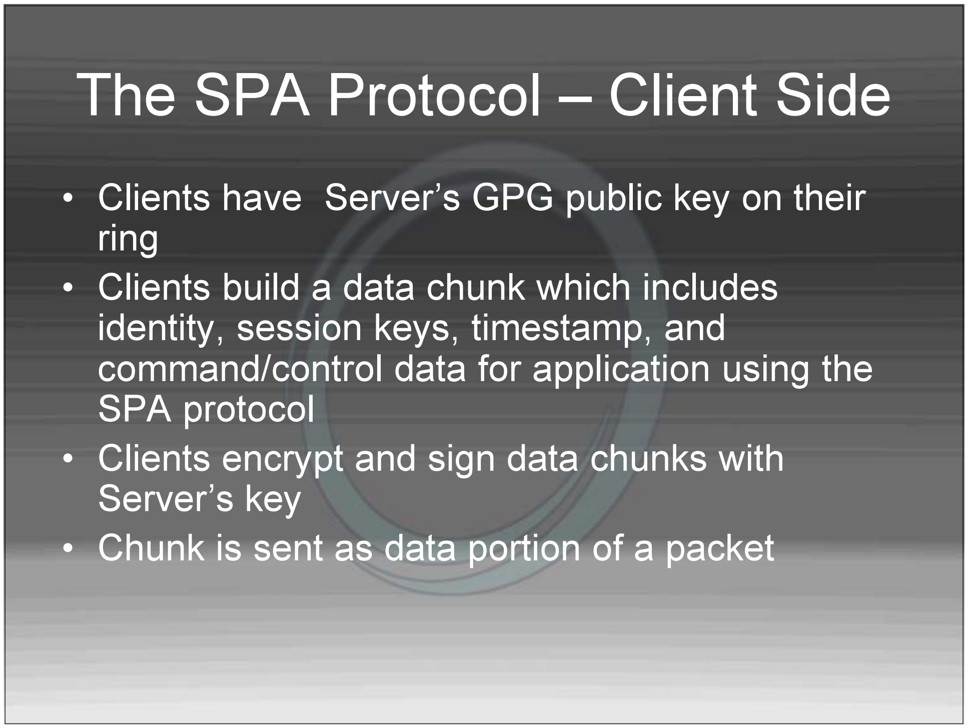
- It is not a replacement for authentication, just another layer
- It is not port knocking, although it can easily replace it with something more secure
- It is not immunity from attacker threats, but it can help immensely by allowing ports to only be opened when necessary

Design Goals

- Free
- Encrypted and signed payload (using GPG/PGP)
- Fairly painless for end user
- Works across NAT
- Uses TCP, UDP, and/or ICMP
- Utilize the PGP Ring of Trust model

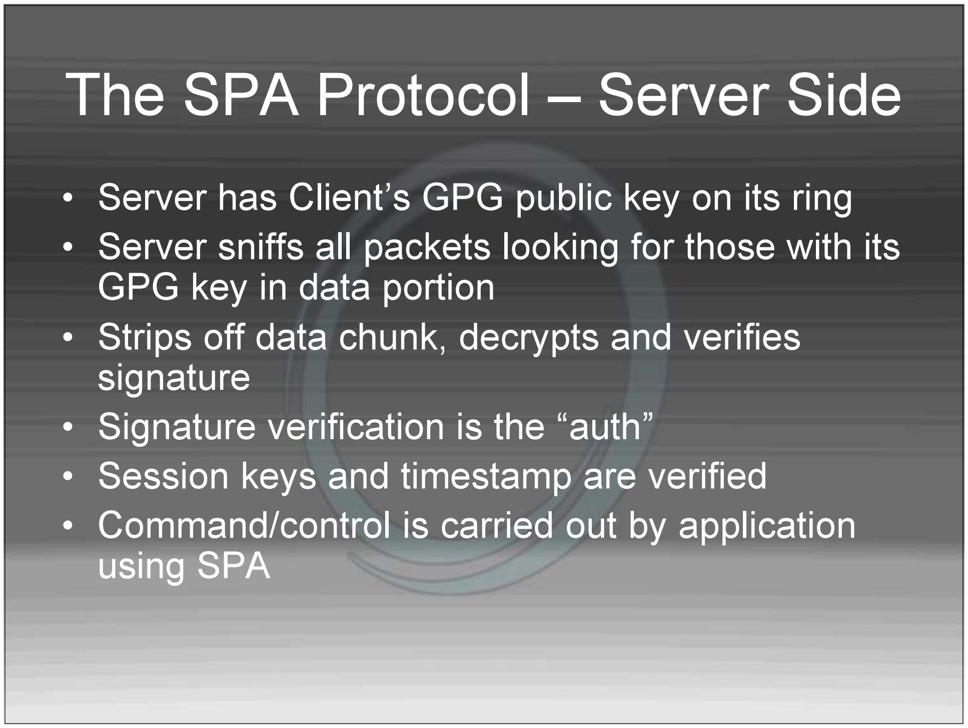


How It Works



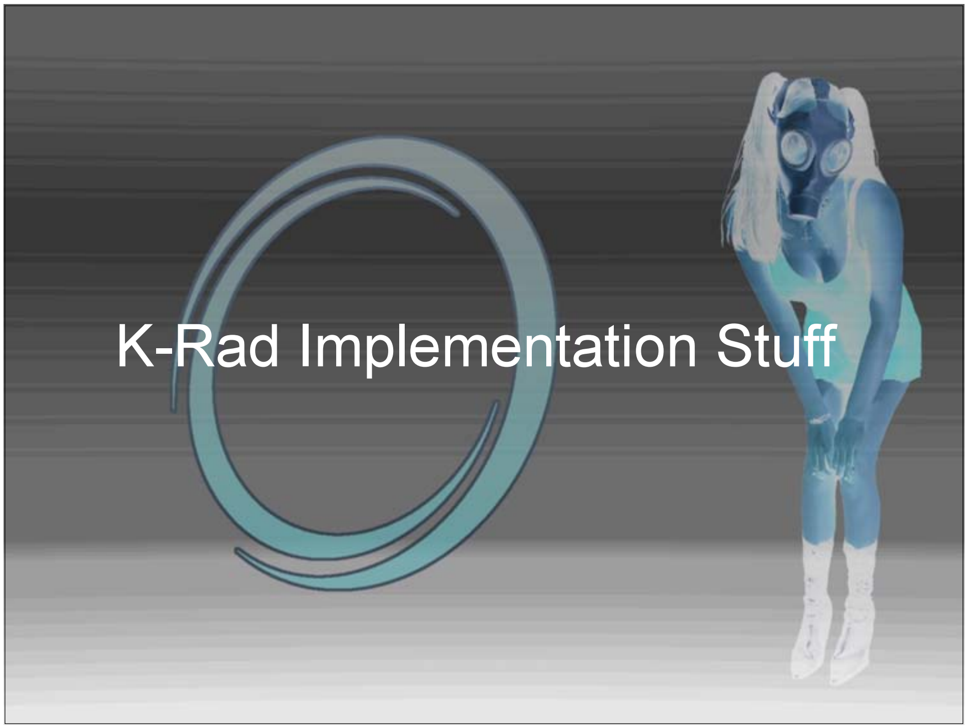
The SPA Protocol – Client Side

- Clients have Server’s GPG public key on their ring
- Clients build a data chunk which includes identity, session keys, timestamp, and command/control data for application using the SPA protocol
- Clients encrypt and sign data chunks with Server’s key
- Chunk is sent as data portion of a packet

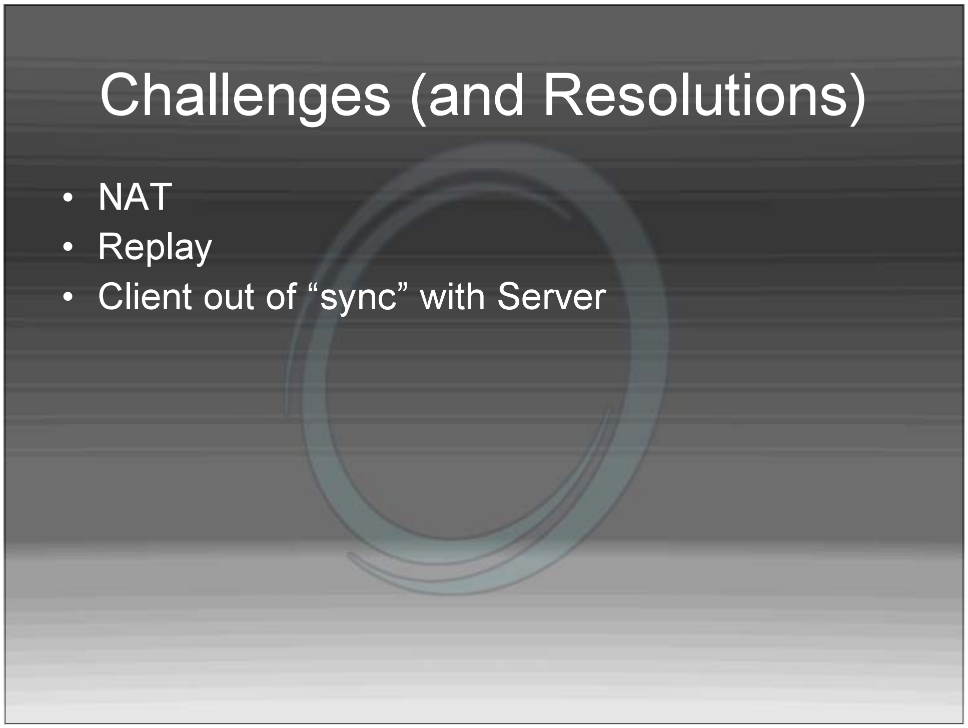


The SPA Protocol – Server Side

- Server has Client’s GPG public key on its ring
- Server sniffs all packets looking for those with its GPG key in data portion
- Strips off data chunk, decrypts and verifies signature
- Signature verification is the “auth”
- Session keys and timestamp are verified
- Command/control is carried out by application using SPA

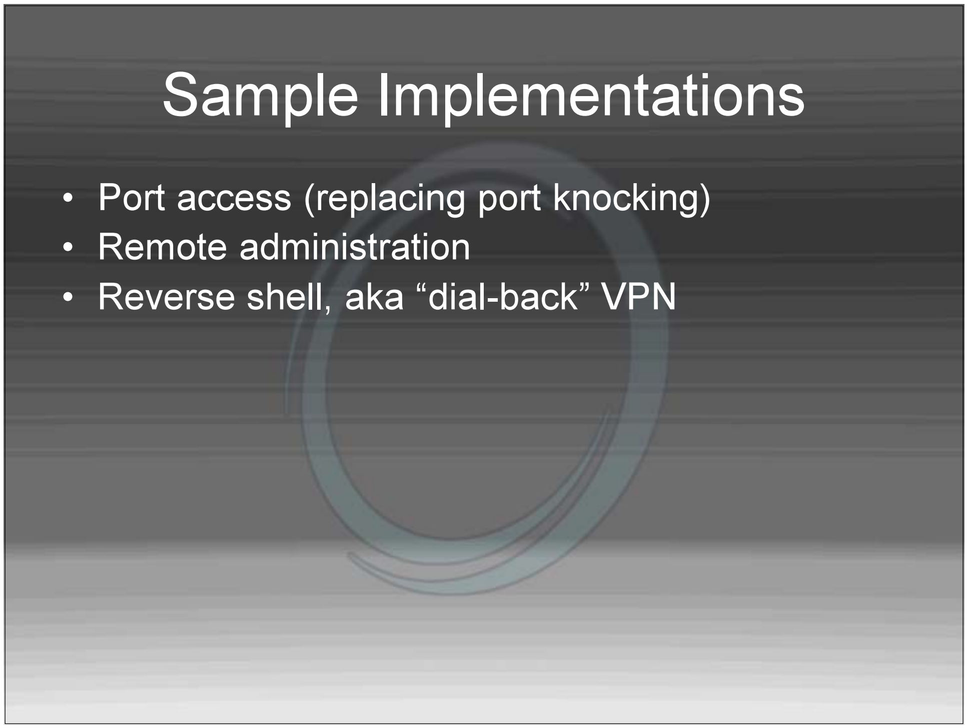


K-Rad Implementation Stuff



Challenges (and Resolutions)

- NAT
- Replay
- Client out of “sync” with Server



Sample Implementations

- Port access (replacing port knocking)
- Remote administration
- Reverse shell, aka “dial-back” VPN

Neato Code to Start Playing With

- Remote firewall administration
- Remote script execution and/or commands

A Quick Psuedo Demo….

FIN

- Thanks!
- Thanks for ideas and help to Druid, all the DC214 guys, Jon Callas for the “dial back” VPN idea, Weasel for art manipulation, and the rest of NMRC
- Photo session by Dui Nguyen and Amy Lee Muir
- NMRC Fetish Model – Bethany
- http://www.unspecific.com/spa/
- spa@nmrc.org

Bad packet, naughty packet…

Images © 2005 NMRC
www.nmrc.org