Building Security at Scale

PRESENTED BY Alex Stamos | Black Hat USA 2014 | August 7, 2014
Agenda

- The Security Industry and Web Scale Problems
- Combating Security Nihilism
- What is Yahoo doing about it?
Theses

- The security industry has failed to consider the needs of scale, including diversity of user base

- A post-Snowden nihilism is affecting our industry’s approach to securing users

- Enterprise security teams need to evolve to proactively gain trust
The Security Industry and Web Scale Problems
What do I mean by scale?

- Amount of
  - Data
  - Systems
  - Users

- Diversity of
  - Users
  - Threat Models
Who is the prototypical customer of security products?
<table>
<thead>
<tr>
<th></th>
<th>Big Banks</th>
<th>Web Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customers</td>
<td>x 10</td>
<td>x 10</td>
</tr>
<tr>
<td>Concurrent Users</td>
<td>x 10</td>
<td>x 10</td>
</tr>
<tr>
<td>Front-End Servers</td>
<td>x 10</td>
<td>x 10</td>
</tr>
<tr>
<td>Total Servers</td>
<td>x 10</td>
<td>x 10</td>
</tr>
<tr>
<td>Customer Value</td>
<td>$100’s</td>
<td>$.01s</td>
</tr>
<tr>
<td>Cust Stickiness</td>
<td>High</td>
<td>Low-Medium</td>
</tr>
<tr>
<td>Meat-Space Identity</td>
<td>Strong</td>
<td>Weak</td>
</tr>
<tr>
<td>Post-Facto Action?</td>
<td>Yes</td>
<td>Rarely</td>
</tr>
</tbody>
</table>
Most security companies are aiming for this

Our reality is more like this

[1] Flickr user Kevin Gebhart CC BY-NC-SA 2.0
[2] Flickr user Dan Buczynski CC BY-NC-ND 2.0
Things People Try to Sell Us
What they try to sell us:

Super smart pizza boxes

What we would buy:

Software sensors with centralized intelligence

[1] Flickr user ms.akr CC BY 2.0
[2] Flickr user Mike Fleming CC BY SA 2.0
Arista 7508E
1152 x 10GbE
30Tbps backplane
5kW

Palo Alto 7050
120Gbps throughput
2.4kW
What they try to sell us:

Databased back SIEM

Hadoop based anomaly detection

What we would buy:

Flickr user Bob Mical [CC BY 2.0]
What they try to sell us:

Windows Anti-APT
Virtualization or
Kernel Firewall

What we would buy:

Docker HIDS

[1] Flickr user broterham CC BY NC 2.0
Free Business Ideas

- Freemium Key Management System
  - Bootstrap via manual approval, trust in network, or remote attestation
  - Create master cert, view into corporate keyspace with lazy security checks

- Freemium Overlay Network
  - Goes great with key manager!
  - Allow for easy IP management across public/private cloud
  - Could be IPv6 only. Terminate inside of containers?

- Bug Bounty with Automatic Verification
  - We’re building this ourselves with Selenium
More Free Ideas

- ARM CoreOS Servers with Lightweight Remote Attestation
  - ARM is going to be big in Big Data environments
  - At scale building systems remotely is currently terrifying
  - Any scale organization does not have 100% physical control

- OpenSSL with Remotable Handshake
  - Why are we putting private keys on the most exposed systems?
  - Need to remote the handshake to an HSM or TXT backed key server
  - Should get 20:1 ratio
Breaking through the excuses
Security Nihilism

Ve believe zat nothing... ist secure enough vor ze real world, Lebowski!

[1] Flickr user Joe Goldberg CC BY-SA 2.0
“Your system is not secure against this [advanced attack|unlikely scenario] therefore it shouldn’t exist”

We need to build systems for all levels of user and adversary

“That’s just security through obscurity!”

Non-obvious protections can increase the chance of catching an attacker in time, especially for interactive systems
“The [NSA|FSB|PLA] will just own up the user’s system and get the data that way”

Forcing an adversary to expend resources and risk detection is a valid goal

“Users are idiots and will screw this up”

A system is only secure if it is safe, by default, for the 25th percentile user
What are we doing about it?
The New Yahoo Paranoids

- CISO
- Chief of Staff
- Corp Security
- Operations and Monitoring
- Product Security Engineering
- Paranoid Labs
- Penetration Testing
- Intelligence, Investigations and Response
- Risk and Vulnerability Management
- Privacy Engineering
Transport Encryption

Complete

› TLS 1.2
› ECDH(E)
› AES-GCM
› RSA 2048

Next up

› HSTS and pre-load
› ECDSA certificates
› Certificate Transparency
› ChaCha20 and Poly1305
› STARTTLS Pinning
Backbone Encryption
Self-Service Security

- Our scaling challenges in providing app sec services:
  - Breadth: 80+ products in 60+ countries
  - Speed: multiple daily web pushes and weekly mobile

- Any large org needs to create self-service options
  - Mobile libraries
    - Authentication and device identity
    - TLS with pinning
  - Mobile code scanning portal
  - CI/CD Scanner integration
    - Open-source coming!
Bug Bounty
Bug Bankruptcy

- Important factors in getting bugs closed:
  - Detailed descriptions and mitigation instructions
  - Accurate prioritization
  - Consistent follow-up and real-time reporting
  - Executive visibility
  - Convincing company that you are a madman

Works well for me
Thanks
Yahoo Parasites
The Future is Bright

- Our profession has never been so impactful on...
  - Individuals
  - Nation-States
  - History

- With great power...
  - It is impossible to work in this field without being a moral actor

- Remember that trust is more than security!

- Take this opportunity to do something that you will remember with pride
Thank you

stamos@yahoo-inc.com