GOING UNDETECTED:
HOW CYBERCRIMINALS, HACKTIVISTS, AND NATION STATES MISUSE DIGITAL CERTIFICATES

Kevin Bocek
The Future: Machines
The future is machines
Adversaries exploiting machine identities
Good news: guidance exists
• Reduce risk
• Build in agility
• Respond faster
What Are Machines?

Device  Code  Algorithm  Service

\[ v = \text{argmax}_{b \in \{\text{Yes, No}\}} \Pr(b) Q_i \Pr(a_i | b) \]
SOFTWARE AND DEVICES EXPLODING
(EST. IN BILLIONS)
An entity without an identity cannot exist because it would be nothing

Aristotle
Law of Identity
*Metaphysics*, Book IV, Part 4
Machine Identities
HUMANS
User name, Password, Biometric

MACHINES
1 0 1 0
0 1 0 1
0 1 0 1
What are Machine Identities?

- SSL/TLS Certificates
- SSH Keys
- API Keys
- Code Signing Certificates

TwL2iGABf9DHoTf09
kqeF8tAmbihY
Role & Lifecycle Leaves Identities Vulnerable

- SSH key for cloud-to-cloud DevOps orchestration
- Code signing certificate to authenticate code running on IoT device
- TLS certificate to authenticate cloud app to IoT devices
Misuse of Machine Identities

- **TAKE ON TRUSTED IDENTITY**
  - Phishing effectiveness
  - Malicious code execution

- **ESTABLISH TRUSTED IDENTITY**
  - Create backdoors
  - Build privilege

- **RUN WITHOUT IDENTITY**
  - Hide, stealth, cloak
Problem: Machine Identities?
Microsoft's Azure service hit by expired SSL certificate

The company also reported service problems with Xbox Music and Video Store services

By John Ribeiro
16,500 Unknown Keys & Certificates Found

On average, IT security professionals found 16,543 additional keys and certificates using Venafi that were previously unknown.

Source: TechValidate survey of 47 Venafi users
Would your organization tolerate 24,000 user IDs & passwords with no awareness, policies, or control?
Would your organization tolerate 24,000 user keys & certificates with no awareness, policies, or control?
Heartbleed: T+1 Year

RED = % NOT HEARTBLEED REMEDIATED
Take On Trusted Identity
Mehr Fahrspaß!
Lenker, Griffe, Tacho & Co.

Top-Marken bei Louis
25M certificates
Let's Encrypt Hands Out 15,000 Fraudulent Security Certificates to Phishers

In the span of a year, Let's Encrypt managed to make people across the Internet feel safe on phishing sites.

Mar 27, 2017 22:23 GMT • By Gabriela Vatu • Share: 📚 ⏩ 🌐 ✍️

Let's Encrypt, a free and open Certificate Authority, has issued close to 15,000 certificates containing the term "PayPal" for phishing sites.

The discovery was made by encryption expert Vincent Lynch, who says 96.7% of the 15,270 security certificates featuring the term "PayPal" issued by Let's Encrypt in the past year have been for phishing sites. The highest density of certificates was issued starting in November 2016. data shows.
“Stealing Certificates will be the Next Big Market for Hackers”
Up to $980/ea

400x more valuable than stolen credit card or identity #
Establishing a trusted identity
APPENDIX F: APT1 SSL CERTIFICATES

The following configured APT1 SSL certificates are used by APT1 to encrypt malware communications using SSL. Detection of these SSL certificates can help to identify APT1 malware infections.

VIRTUALWEB

<table>
<thead>
<tr>
<th>Certificate Authority</th>
<th>Common Name</th>
<th>Serial Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec</td>
<td><a href="http://www.virtualweb.com">www.virtualweb.com</a></td>
<td>9876543210</td>
</tr>
<tr>
<td>Verisign</td>
<td>virtualweb.example.com</td>
<td>0987654321</td>
</tr>
<tr>
<td>Comodo</td>
<td>virtualweb.com</td>
<td>9087654321</td>
</tr>
</tbody>
</table>

For the full report visit http://www.mandiant.com/apt1
As you can see in Figure 4, this version of Dropbear SSH will authenticate the user if the password passDs5Bu9Te7 was entered. The same situation applies to authentication by key pair – the server contains a pre-defined constant public key and it allows authentication only if a particular private key is used.

Figure 5 – The embedded RSA public key in SSH server

Every business and government has the same lack of awareness and control over SSH keys.
Run Without An Identity
SSL/TLS
Encrypted Tunnel
“70% OF MALWARE ATTACKS WILL USE SSL BY 2020”
LESS THAN 20%

Of Organizations with a FW, IPS/IDS, or UTM decrypt SSL/TLS traffic
16,500 Unknown Keys & Certificates Found

On average, IT security professionals found 16,543 additional keys and certificates using Venafi that were previously unknown.

Source: TechValidate survey of 47 Venafi users
BLIND TO ATTACK

One Unknown Certificate

= Encrypted tunnel

= Can’t see what’s coming
Weaponizing Machine Identities

**2010-2012**
- **Attacks Begin**
  - 2010: Blueprint - Stuxnet and Duqu
  - 2011: CAs Attacked
  - 2012: Online Trust Questioned by Experts

**2013**
- **Attacks Become Mainstream**
  - SSH & server key theft
  - Code-signing certificate theft
  - MITM by CA compromise

**2014**
- **Advanced Campaigns Launch**
  - Targeted key & certificate theft
  - Sold on Underground
  - Multi-year campaigns
  - SSL & SSH vulnerabilities

**2015**
- **Online Trust Crumbles**
  - Price increases on underground
  - Digitally-signed malware doubles quarterly
  - SSL/TLS used to hide activity
  - MitM attacks
  - SSH pivoting

**2016-2017**
- **Threatscape Expands**
  - SSL/TLS used to bypass security
  - Encrypt Everywhere grows attack surface
  - SHA-1 deprecation
  - SHA-1 collision successful
Preparing Your Plans
Better Safe Than Sorry: Preparing for Crypto-Agility

Published: 30 March 2017    ID: G00323310

Analyst(s): Mark Horvath, David Anthony Mahdi

Sudden and unpredictable algorithmic and cryptographic vulnerabilities can leave application owners scrambling. Security leaders and enterprise readers
must prepare themselves for generating agile response plans.

Key Challenges
- Cryptographic algorithms break suddenly, at least from an end-user point of view.
- Most IT organizations are not aware of the type of encryption they are using, which applications are using it or how it is used.
- Developers are often blind to the details of cryptographic and hash function libraries and sometimes hard-code dependencies. This can make patching or incidence response difficult or unpredictable.
- Open-source algorithms are often viewed as safe because of their constant public exposure, but actual implementation reviews are rare.

Recommendations
- Security should be the first consideration for all new applications, especially those related to storing or transmitting sensitive data.
- Implement a robust patching and vulnerability management program to ensure that all systems are up-to-date and secure.
- Conduct regular security audits and penetration testing to identify and address potential vulnerabilities.
- Train developers on secure coding practices and encourage them to use established cryptographic libraries instead of implementing their own.
Crypto-agility

Recommendations

Security and risk management leaders responsible for application security:

- Build crypto-agility into application development or application procurement workflow. Ask vendors specifically about how security incidents are communicated and who is responsible for incident response.

- Inventory the applications that use cryptography, thereby evaluating your dependence on such algorithms. This will give your organization a way to scope the impact of a break, and allow you to determine the risk to specific applications and prioritize incident response plans accordingly.

- Include cryptographic alternatives and an algorithm swap-out procedure in your incident response plans.
ITL Bulletin for July 2012

Preparing for and Responding to Certification Authority Compromise and Fraudulent Certificate Issuance

Paul Turner, Venafi

William Polk, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce

Elaine Barker, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce

1. Executive Summary

As the use of public key infrastructure (PKI) and digital certificates (e.g., the use of transport layer security (TLS) and secure sockets layer (SSL)) for the security of systems has increased, the certification authorities (CAs) that issue certificates have increasingly become targets for sophisticated cyber-attacks. In 2011, several public certification authorities were attacked, and at least two attacks resulted in the successful issuance of fraudulent certificates by the attackers. An attacker who compromises a CA to generate and obtain fraudulent certificates does so to launch further attacks against other organizations or individuals. An attacker can also use fraudulent certificates to authenticate as another individual or system or to forge digital signatures.

These recent attacks on CAs make it imperative that organizations remove all associated trust in CAs and must also be prepared to detect and respond to the issuance of fraudulent certificates.
Find What’s Out There

Set, Enforce a Policy

Automate Response

Good News: this can be business as usual process
Roadmap: Control of Machine Identities

Level 0: Chaos
Have unquantified security risk, outages, expensive and manual processes, and compliance challenges

Level 1: Control
Build a security foundation with focus on known and trusted keys and certificates

Level 2: Critical Systems
Secure and protect all keys and certificates on business-critical infrastructure

Level 3: Enterprise Protection
Protect and automate all keys and certificates enterprise-wide and further reduce costs and extract more business value

Level 4: Machine Identity Protection
Rapidly respond to internal and external threats and security incidents related to keys and certificates

Endpoint/Mobile
Virtual Machines
Cloud
Start Change

- Who is responsible?
- How do we enforce policies?
- How do we monitor Let’s Encrypt and other CAs?
- How will we automate for IoT, DevOps, cloud?
- How would we respond to?
  - CA compromise
  - SSH key theft
- And keeping asking more...
GOING UNDETECTED:
HOW CYBERCRIMINALS, HACKTIVISTS, AND NATION STATES MISUSE DIGITAL CERTIFICATES
Kevin Bocek
Keys and Certificates
Are the Foundation of Your Security Infrastructure

• SSL/TLS Encryption
• WiFi & VPN Access
• Cloud
• DevOps
• Mobility
• Internet of Things
• SSH Privileged Access