• Cyber space is very similar to organic realm
• Keys & certificates are like HLA tags
• But, we don’t have an active or adaptive immune system
• Trust seems “blind”
• Did we really solve the first Internet security problem?
"On the Internet, nobody knows you're a dog."
Building Layered Security
When the Foundation Isn’t Protected
Weaponization of Keys and Certificates

**2010**
Stuxnet and Duqu demonstrate powerful weapon

**2011**
Attackers open new front with assault on Certificate Authorities

**2012**
Can any key or certificate be trusted?

**2013**
Mainstream usage as an attack vector

**2014**
Advanced campaigns

**2015**
Broken Trust

**Blueprints**
- Stuxnet and Duqu demonstrate powerful weapon
- Attackers open new front with assault on Certificate Authorities
- Can any key or certificate be trusted?

**Uping the ante**
- SSH Key Theft
- CA Compromise to Enable “MITM” Attacks
- Server Key Theft
- Weak Crypto Exploits
- Code Signing Certificate Theft

**2010 - 2011**
- SSH Key Theft
- CA Compromise to Enable “MITM” Attacks
- Server Key Theft
- Weak Crypto Exploits
- Code Signing Certificate Theft

**2012 - 2013**
- SSH Key Theft
- CA Compromise to Enable “MITM” Attacks
- Server Key Theft
- Weak Crypto Exploits
- Code Signing Certificate Theft

**2014 - 2015**
- 100% Responded to Attacks
- Certificate Price Increase on Underground
- Digitally-signed Malware Doubling Every Quarter
- SSL & SSH Vulnerabilities
- Sold on the Underground Market
- Own the Network
- Multi-year Campaigns

**2010 - 2015**
- Digitally-signed Malware Doubling Every Quarter
- TLS Used to Hide Activity
- MITM Attacks

Lucky13
Heartbleed

- Vulnerability in OpenSSL
- Enables extraction of data without a breach
- SSL/TLS Keys and certificates **must** be assumed compromised
Patch vulnerable OpenSSL systems

Assume ALL keys and certificates compromised

Must generate new keys and certificates

Validate changes to demonstrate remediation
Global 2000: Heartbleed Remediation

April 2015

Australia: 16% Remediated, 84% Not Remediated
France: 22% Remediated, 78% Not Remediated
Netherlands: 32% Remediated, 68% Not Remediated
UK: 33% Remediated, 67% Not Remediated
US: 41% Remediated, 59% Not Remediated
Germany: 42% Remediated, 58% Not Remediated
25,540 KEYS & CERTIFICATES
On average per company

UP 40% FROM 2013
18,351

$1000 PRICE TAG
For a stolen certificate in the underground marketplace
“Stealing Certificates will be the Next Big Market for Hackers”
Marketplace for Stolen Certificates

Up to $980/ea

400x more valuable than stolen credit card
3x more valuable than bitcoin
Underground Certificates-as-a-service (CaaS)

Some of the certificates for sales were issued for 1 year, which is enough for targeted APT.
Bad actors actively use legitimate certificate authorities to issue digital certificates for malware.

InfoArmor: GovRAT
Total Malicious Signed Binaries

- Q3 2013
- Q4 2013
- Q1 2014
- Q2 2014
- Q3 2014
- Q4 2014
- Q1 2015
- Q2 2015
Our concern with a CA’s unfettered authority to issue certificates is heightened when the CA is owned and operated by a government. Because digital certificates are used to ensure the security and confidentiality of private communications like e-mail and social media, such services can be targets for actors who wish to inhibit political freedoms such as free expression.

misuse of certificates is a danger to global economy
trusted: in your computer, browser, smartphone, server
Example: MCS Holdings, an intermediate CA for CNNIC issued a fraudulent certificate for Google to perform Man-in-the-Middle

Security risks from untrustworthy CAs like CNNIC?

- 58% Don't know
- 22% MITM attacks
- 14% No risk
- 6% Replay attacks

Browser action to protect you

- Untrusted by Google
- Untrusted by Mozilla
- Trusted by Apple
- Trusted by Microsoft

Venafi: Black Hat 2015 survey
February 16, 2016

A Message to Our Customers

The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand.

This moment calls for public discussion, and we want our customers and people around the country to understand what is at stake.

The Need for Encryption

All that information needs to be protected from hackers and criminals who want to access it, steal it, and use it without our knowledge or permission.

Compromising the security of our personal information can ultimately put our personal safety at risk. That is why encryption has become so important to all of us.
In today’s digital world, the “key” to an encrypted system is a piece of information that unlocks the data, and it is only as secure as the protections around it. Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge.

The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers — including tens of millions of American citizens — from sophisticated hackers and cybercriminals. The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe.

We can find no precedent for an American company being forced to expose its customers to a greater risk of attack. For years, cryptologists and national security experts have been warning against weakening encryption. Doing so would hurt only the well-meaning and law-abiding citizens who rely on companies like Apple to protect their data. Criminals and bad actors will still encrypt, using tools that are readily available to them.
What action did your organization take after CNNIC was deemed untrusted?

74% remain exposed

- 34% Wait for Microsoft and Apple to take action
- 26% Remove CNNIC from all desktops, laptops, and mobile devices
- 23% No action was taken
- 17% Don't know

Venafi: Black Hat 2015 survey
Awareness Visibility Detection

Blind Spot in Security

- Keys & Certificates
- Encryption
- AV
- VPN
- MDM
- Firewall
- DLP
- IDS
- IAM
- IPS

Awareness Visibility Detection

Ability to respond
How much network traffic will be encrypted?

This Memorandum requires that all publicly accessible Federal websites and web services only provide service through a secure connection. The strongest privacy and integrity protection currently available for public web connections is Hypertext Transfer Protocol Secure (HTTPS).
“50% of network attacks will use SSL by 2017”

Gartner
Undermines Security
“Basically, the enterprise is a sitting duck.”
Customer Problems we Find

Our network is down – certificate expired

We can’t decrypt all inbound traffic – we don’t have the keys

What’s on the network?? we just found 50,000 self-signed certificates

Marketing purchased 50 certificates to improve SEO

We can’t decrypt all inbound traffic – we don’t have the keys

Our network is down – certificate expired

What’s on the network?? we just found 50,000 self-signed certificates

Application Owner
PKI Owner
Business Owner
millions of certificates

GLOBAL TELCO

millions of certificates
Consequences of the Problems we Find

We have **no visibility** in to certificates outside the firewall.

We can’t securely collect and transfer keys to security systems.

We’re unable to continuously monitor and remediate automatically.

We can’t enforce policy and detect anomalies.

Application Owner
PKI Owner
Business Owner
Where to Start?

RECOMMENDATIONS

- Document and enforce policies, like revocation processes
- Secure keys as a ‘top priority’
- Monitor security feeds for compromised CAs and certificates
- Survey and monitor all certificates
SANS - 20 Critical Security Controls

- Inventory of Devices
- Secure Configurations
- Application Software Security
- Data Recovery Capability
- Control of Network Ports, Protocols, Services
- Maintain, Monitor, and Analysis Of Audit Logs
- Secure Network Engineering
- Penetration Tests and Red Team
- Incident Response & Management
- Malware Defense
- Continuous Vulnerability Assessment
- Wireless Access Control
- Security Skills Assessment And Training
- Controlled Use of Administrative Privileges
- Controlled Access
- Account Monitoring And Control
- Data Protection
- SANS - 20 Critical Security Controls
CSC17 Update

✓ Know what’s out there
✓ Does it fit with policy
✓ If not, fix it
✓ Establish ownership
✓ Automate & Repeat
Venafi TrustAuthority & Venafi TrustNet: Visibility and Control

1. Internet-wide Discovery
   - Establish Inventory, Gain Visibility
   - Certificate reputation
   - Notify on anomalies

Cloud

2. Enroll and Revoke
   - Understand and Fix Vulnerabilities
   - External CA #1
   - Internal CA

3. Set Policy, Workflow & Notification
   - Establish Norms
   - Validate Baseline
   - SSH Discovery
   - Network Discovery

4. Application Owner
   - Assign Roles, Secure Self-Service
   - Self Service Portals / API

5. Business Owner
   - Monitor & ID Anomalies
   - Reporting/Analysis
   - CA Import
   - Reporting/Analysis

For all SSL, SSH, Mobile keys and certificates
Venafi TrustForce & Venafi TrustNet: Rapid Response and Remediation

1. Respond
2. Scale
3. Powerful Automation
4. Install, Configure and Validate

- Install Certs and Rotate Keys on Demand (Physical, Virtual, Cloud)
- Post Install: App Configuration and Validation
- Build Associations between Applications and Certificates
- Monitor Trust Bundles, SSH Keys, and Users
- Take Action from Alerts and Notifications

For all SSL keys/certificates and SSH keys
Lessons from Human Immune System
• Keys and certificates can’t be blindly trusted
• We have to actively inspect, constantly adapt
• Find keys certificates, trusted?, fix, securely distribute and scale