Security in knowledge

Controlling Trust and Risk

Craig Marois

The Boeing Company

Larry Ponemon

The Ponemon Institute

RSA CONFERENCE 2013

Session ID: SPO1-R35

Session Classification: Intermediate

“All the world is made of faith, and trust, and pixie dust.”

– J.M. Barrie

Public Key Infrastructure

- **What do we use PKI for?**
  - **Encryption** (PGP, S/MIME)
  - **Authentication** (Users, devices, documents, Smartcard logon, SSL client auth, XML signatures)
  - **Bootstrapping** secure communications (IKE, SSL)
  - **Code Signing**
- **Establishing a trusted PKI provides a keystone to building a secure and trusted data communications framework**

PKI and Trust

- **PKI + Trust = Assurance**
- **PKI – Trust = Overhead + Liability**
  - Therefore **Trust** is the critical component of an effective and viable PKI
- **So how do we establish trust?**
  - Policy – These are our assertions
    - Certificate Policy
    - Certification Practice Statement
    - Key Recovery Practice Statement
  - Auditing – This is how we prove that we do what we say
    - Independent
    - Internal
  - Standards?

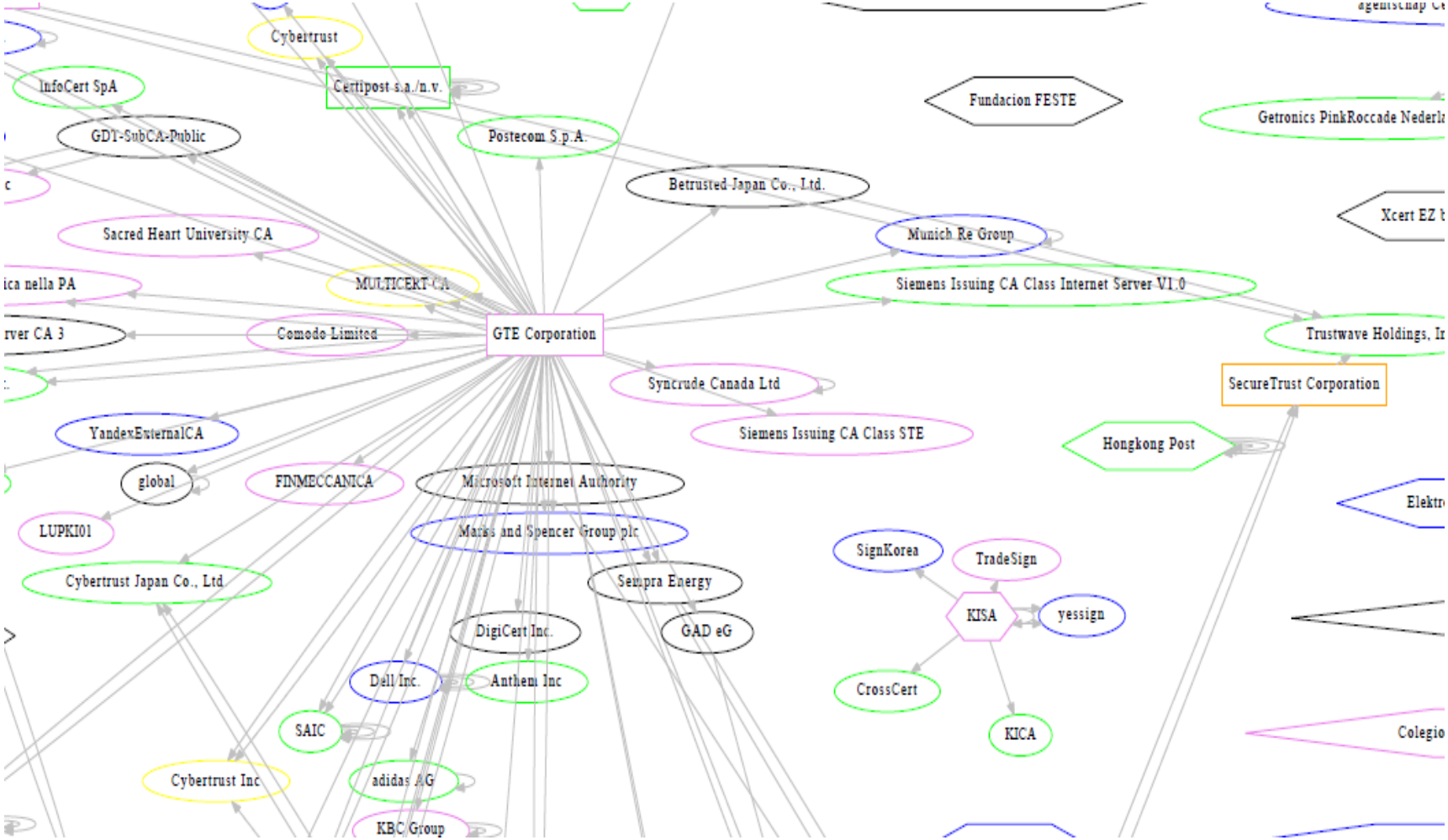
Policies

- **Two specific polices are critical:**
  - **Certificate Policy** (CP)
    - Describes the components and actors within the PKI and what each component's specific roles and responsibilities are
  - **Certificate Practice Statement** (CPS)
    - Describes the practices related to issuance, renewal, revocation, publication, and archiving of certificates

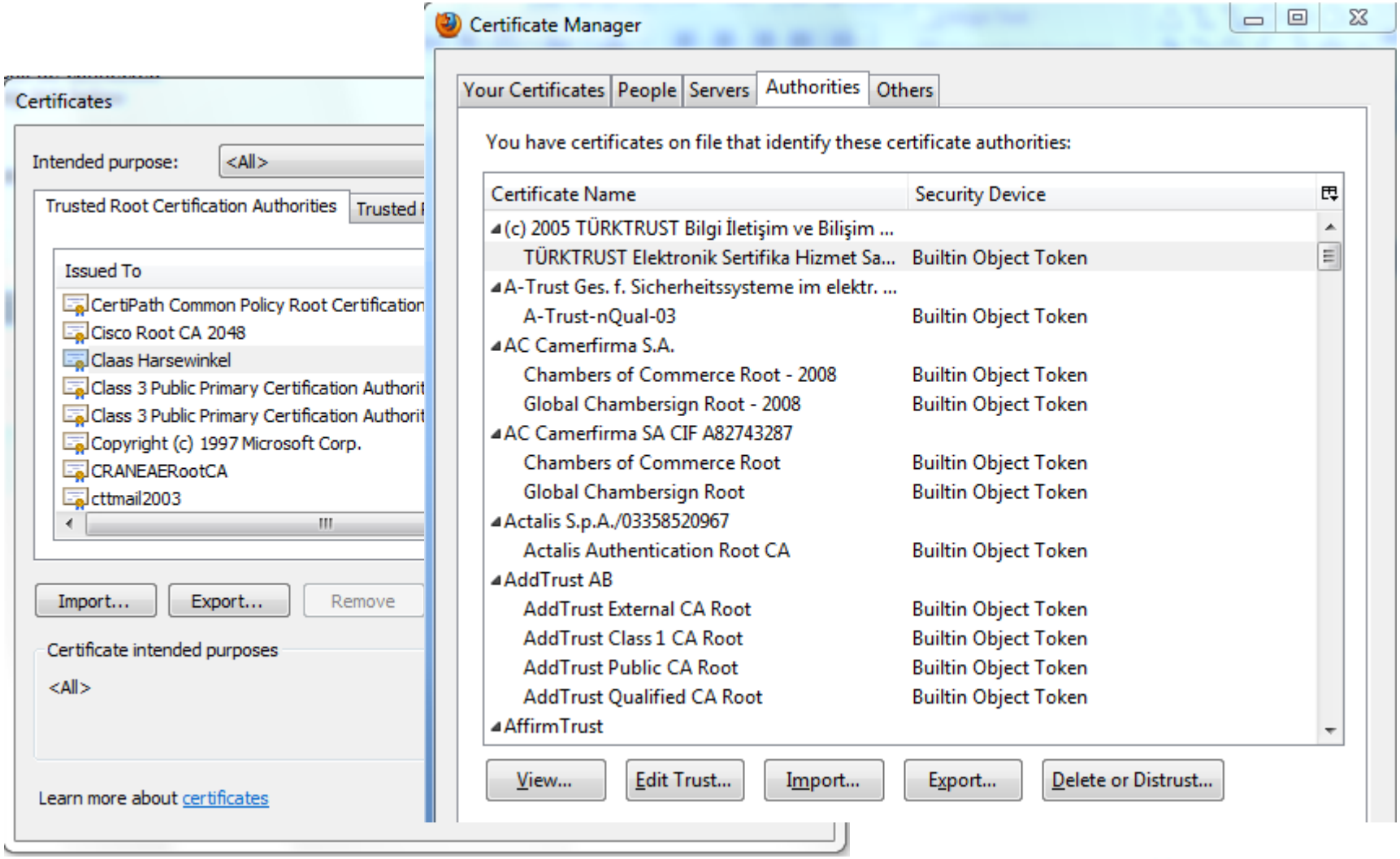
So Who Do We Trust?

- **Just about everyone….**
- **The Electronic Frontier Foundation's (EFF) SSL Observatory project**
  - Investigates the use of SSL/TLS on the Internet
  - Mapped the 650 plus CA's that are trusted directly or indirectly by Internet Explorer and/or Firefox
    - Are all of these CA's secure?
    - How would we ever know?

Who Do We Trust?



Who Do We Trust?



PKI Attacks

One bad apple spoils the bunch!

- Browsers explicitly trust many "public" CA's by default, so if one of these CA's is compromised, everyone who uses a web browser is at risk
- Comodo
- DigiNotar
- TURKTRUST

DigiNotar Attack

- **DigiNotar *was* a Dutch certificate authority**
  - Trusted CA in many popular browsers
  - Issued certificates for the Dutch government
- **In the summer of 2011, 531 fraudulent certificates were issued from DigiNotar's PKI**
  - *.google.com certificate was subsequently used in a man-in-the-middle attack in Iran
- **Attacker operated without DigiNotar's knowledge for over a month.**
- **After the breach was recognized, DigiNotar did not immediately notify users of the breach**

DigiNotar Attack

- **Timeline**
  1. First sign of the attack June 17th 2011
  2. DigiNotar recognizes the attack July 19th 2011
  3. Users notice fraudulent certificates August 29th 2011
  4. DigiNotar files for bankruptcy September 20th 2011
- **Reputation and trust are essential in the PKI business**

DigiNotar Attack

How did this attack happen?

- Investigation by independent security consultant Fox IT showed the following:
  - Unpatched software
  - Lack of anti-virus protection
  - Weak passwords
  - Multiple CA's on a single domain
  - Poorly tuned IDS/IPS systems
  - CA network remotely accessible from a management VLAN

How do we protect ourselves from risk?

"The three golden rules to ensure computer security are:

- **do not own a computer**
- **do not power it on**
- **and do not use it."**

– Robert Morris, NSA

Protecting PKI

- Fundamentals
  - Patching, including offline CA's
  - Antivirus
  - Auditing
  - Two-factor authentication - Password-only logins are a liability
- Accounts with elevated privileges
  - Audit these accounts frequently
  - Multifactor authentication
- Offline Root CA's
- Hardware-based security
- Host-based intrusion detection systems
  - File integrity checking
    - Access auditing

“One of the most time-consuming things is to have an enemy”

– E.B. White

“Never underestimate the attention, risk, money, and time that an opponent will put into reading traffic.”

– Robert Morris, NSA

Takeaways

- **PKI is not perfect**
  - Browser vendors do not help
  - No real viable alternatives (right now)
    - Potential Alternatives
      - Public Key Pinning Extension for HTTP
      - DNSSEC-TLS
        - Relies on implementation of DNSSEC
      - Convergence
        - Multiple notaries reach a consensus regarding authenticity
- **Public key infrastructures are being targeted**
  - DigiNotar, Comodo, TURKTRUST, Others?

Takeaways

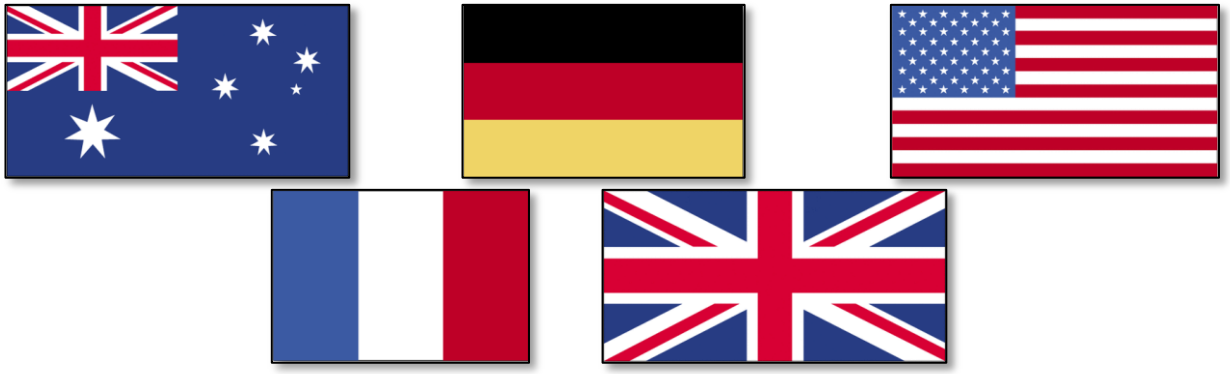
- **Need to take a defense-in-depth approach**
  - Strong perimeter
    - Lock down ports and services
    - Don't build your CA and then build your perimeter around it. Understand your data flows and harden the environment first
  - Strong authentication controls
    - Two factor
      - SmartCards
      - Get rid of username/password logins
  - Host-based intrusion detection systems
    - HIDS can be an effective tool to enforce PKI policies
    - File integrity checking
  - Auditing

Takeaways

- **Plan for the unexpected**
  - What would happen if your CA or your vendor's CA was compromised?
    - Have a revocation and re-issue plan
- **Manage certificates**
  - Implement lifecycle management tools to ensure that certificates do not expire unexpectedly
    - Don't allow certificate expirations to become a liability
  - Understand what types of certificates are issued
    - MD5, SHA-1, etc.
    - Expect that at some point these algorithms will become vulnerable and have a plan to identify and replace them

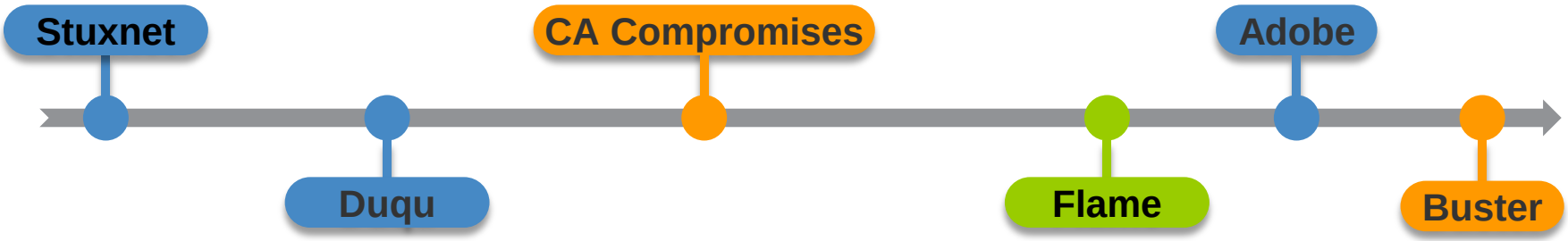
2013 Cost of Failed Trust Report

- ***Threats & Attacks*, first in a series**
- Global research focused on Global 2000



Threats & Attacks

Alarming rise in trust exploits



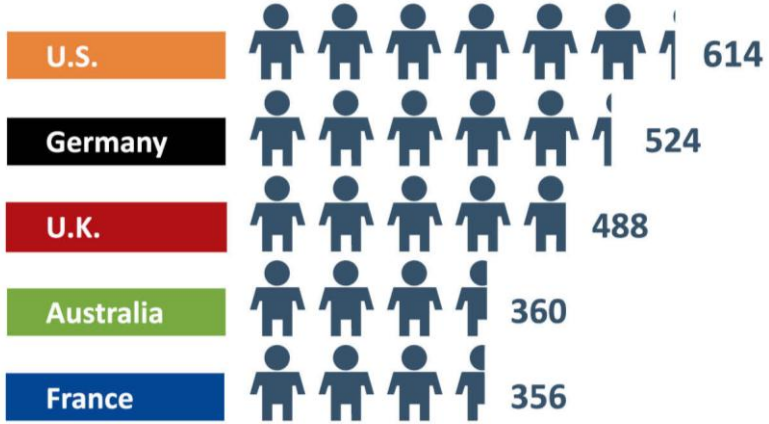
Attackers stole private keys from two Taiwanese companies and Adobe to sign code.

Attackers compromise or dupe certificate authorities to issue fraudulent certificates for further attacks.

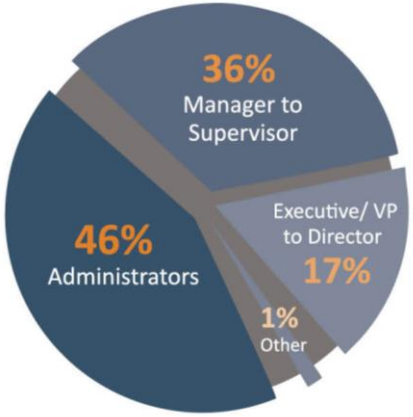
Attackers exploited MD5 to create a face Microsoft CA certificate and then sign code.

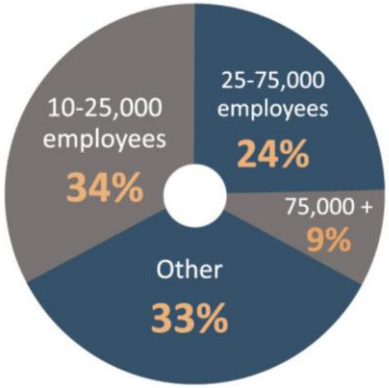
Global Demographics

2,342 survey respondents from within the Global 2000



The Ponemon Institute vetted respondents





Ponemon INSTITUTE

Enterprise Reliance on Keys & Certificates

17,807

Average number of server keys and certificates in a Global 2000 organization

Losing Control Over Trust

51%

Don’t know how many keys and certificates are in use by their organization

Losing Control Over Trust

45%

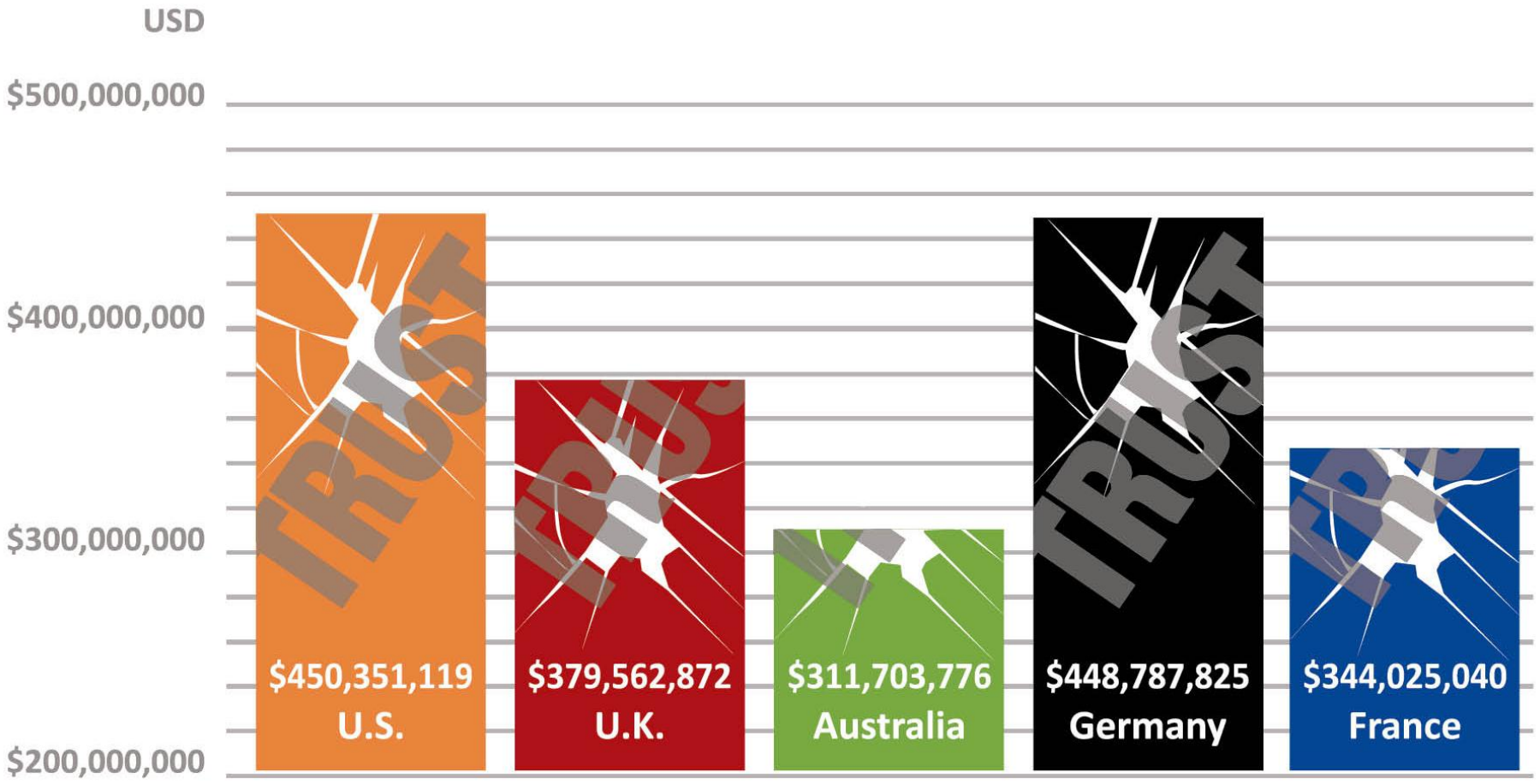
"Failing to manage keys and certificates means losing control over the trust my organization relies upon to operate."

Total Possible Impact of Attacks

$398M

Losses facing every Global 2000 organization from attacks on trust

Total Possible Impact of Attacks



Ponemon INSTITUTE

Impact Already Felt

1 or more

Trust exploits and attacks from key & certificate management failures in every organization over last 2 years

Solving the Problem

59%

Getting key and certificate management right *first*, solves security, operations, and compliance problems of using encryption

Solving the Problem

#1 Most Alarming Key & Certificate Management Threat

SSH

Conclusions

- **Nearing tipping point** where trust exploits are a daily occurrence
- **Little awareness and preparedness**
- Attacks likely to **challenge trust in the cloud**
- **Expect more attention** from auditors and regulators

download full research at www.venafi.com

Security in knowledge