National Strategy for Trusted Identities in Cyberspace

VCAT Discussion | 2.8.2012

Jeremy Grant
NIST
What is NSTIC?

Called for in President’s Cyberspace Policy Review (May 2009): a “cybersecurity focused identity management vision and strategy...that addresses privacy and civil-liberties interests, leveraging privacy-enhancing technologies for the nation.”

Guiding Principles

• Privacy-Enhancing and Voluntary
• Secure and Resilient
• Interoperable
• Cost-Effective and Easy To Use

NSTIC calls for an **Identity Ecosystem**, “an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities.”
The Problem Today

Usernames and passwords are broken

- Most people have 25 different passwords, or use the same one over and over
- Even strong passwords are vulnerable...criminals can get the “keys to the kingdom”
- Rising costs of identity theft
  - 8.1M U.S. victims in 2010 at a cost of $37 billion (Javelin)
- A common vector of attack
  - Sony Playstation, Zappos, Lulzsec, Infragard among dozens of 2011-12 breaches tied to passwords.
The Problem Today

<table>
<thead>
<tr>
<th>Category</th>
<th>Threat Action Type</th>
<th>Short Name</th>
<th>Breaches</th>
<th>Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Malware</td>
<td>Send data to external site/entity</td>
<td>SNDATA</td>
<td>297</td>
<td>1,729,719</td>
</tr>
<tr>
<td>2 Malware</td>
<td>Backdoor (allows remote access / control)</td>
<td>MALBAK</td>
<td>294</td>
<td>2,065,001</td>
</tr>
<tr>
<td>3 Hacking</td>
<td>Exploitation of backdoor or command and control channel</td>
<td>HAKBAK</td>
<td>279</td>
<td>1,751,530</td>
</tr>
<tr>
<td>4 Hacking</td>
<td>Exploitation of default or guessable credentials</td>
<td>DFCRED</td>
<td>257</td>
<td>1,169,300</td>
</tr>
<tr>
<td>5 Malware</td>
<td>Keylogger/Form-grabber/Spyware (capture data from user activity)</td>
<td>KEYLOG</td>
<td>250</td>
<td>1,538,680</td>
</tr>
<tr>
<td>6 Physical</td>
<td>Tampering</td>
<td>TAMPER</td>
<td>216</td>
<td>371,470</td>
</tr>
<tr>
<td>7 Hacking</td>
<td>Brute force and dictionary attacks</td>
<td>BRUTE</td>
<td>200</td>
<td>1,316,588</td>
</tr>
<tr>
<td>8 Malware</td>
<td>Disable or interfere with security controls</td>
<td>DISABL</td>
<td>189</td>
<td>736,884</td>
</tr>
<tr>
<td>9 Hacking</td>
<td>Footprinting and Fingerprinting</td>
<td>FTPRNT</td>
<td>185</td>
<td>720,129</td>
</tr>
<tr>
<td>10 Malware</td>
<td>System/network utilities (PsTools, Netcat)</td>
<td>UTILITY</td>
<td>121</td>
<td>1,098,643</td>
</tr>
<tr>
<td>11 Misuse</td>
<td>Embezzlement, skimming, and related fraud</td>
<td>EMBZZL</td>
<td>100</td>
<td>37,229</td>
</tr>
<tr>
<td>12 Malware</td>
<td>RAM scraper (captures data from volatile memory)</td>
<td>RAMSCR</td>
<td>95</td>
<td>606,354</td>
</tr>
<tr>
<td>13 Hacking</td>
<td>Use of stolen login credentials</td>
<td>STLCRED</td>
<td>79</td>
<td>817,159</td>
</tr>
<tr>
<td>14 Misuse</td>
<td>Abuse of system access/privileges</td>
<td>ABUSE</td>
<td>65</td>
<td>22,364</td>
</tr>
<tr>
<td>15 Social</td>
<td>Solicitation/Bribery</td>
<td>BRIBE</td>
<td>59</td>
<td>23,361</td>
</tr>
</tbody>
</table>

Source: 2011 Data Breach Investigations Report, Verizon and USSS
The Problem Today

Identities are difficult to verify over the internet

- Numerous government services still must be conducted in person or by mail, leading to continual rising costs for state, local and federal governments

- Electronic health records could save billions, but can’t move forward without solving authentication challenge for providers and individuals

- Many transactions, such as signing an auto loan or a mortgage, are still considered too risky to conduct online due to liability risks
The Problem Today

Privacy remains a challenge

• Individuals often must provide more personally identifiable information (PII) than necessary for a particular transaction
  – This data is often stored, creating “honey pots” of information for cybercriminals to pursue

• Individuals have few practical means to control use of their information
Personal Data is Abundant…and Growing

Trusted Identities provide a foundation

- Economic benefits
  - Enable new types of transactions online
  - Reduce costs for sensitive transactions
- Improved privacy standards
  - Offer citizens more control over when and how data is revealed
  - Share minimal amount of information
- Enhanced security
  - Fight cybercrime and identity theft
  - Increased consumer confidence

TRUSTED IDENTITIES
The Identity Ecosystem: Individuals can choose among multiple identity providers and digital credentials for convenient, secure, and privacy-enhancing transactions anywhere, anytime.

- Apply for mortgage online with e-signature
- Online shopping with minimal sharing of PII
- Trustworthy critical service delivery
- Secure Sign-On to state website
- Security ‘built-into’ system to reduce user error
- Privately post location to her friends

January 1, 2016
What does NSTIC call for?

Private sector will lead the effort

- Not a government-run identity program
- Industry is in the best position to drive technologies and solutions
- Can identify what barriers need to be overcome

Federal government will provide support

- Help develop a private-sector led governance model
- Facilitate and lead development of interoperable standards
- Provide clarity on national policy and legal framework around liability and privacy
- Act as an early adopter to stimulate demand
NSTIC National Program Office

• Charged with leading day-to-day coordination across government and the private sector in implementing NSTIC

• Funded with $16.5M for FY12
Key 2012 NSTIC Implementation Activities

1. Establishment of the Identity Ecosystem Steering Group
   - NIST Recommendations to be published mid-February
   - New 2-year grant to fund a privately-led (.com or .org) Steering Group to convene stakeholders and craft standards and policies to create an Identity Ecosystem Framework

2. NSTIC Pilots Grant Program
   - FFO recently published for $10M NSTIC pilots grant program
   - 5-8 awards expected by late summer
   - Focus on addressing barriers the marketplace has not yet overcome
   “Make something happen that otherwise would not”
Key 2012 NSTIC Implementation Activities

3. Buildout of NPO
   - Hire key staff (tech, privacy, governance, pilots leads)
   - Model: influence via active engagement in Steering Group and managing pilots

4. Coordinate Federal efforts for .gov adoption
   - Government agency embrace of NSTIC is key to convincing non-governmental stakeholders that the Strategy is viable
   - Identifying agencies with potential killer apps and willingness to be early adopters
We've proven that Trusted Identities matter

DoD Led the Way

• DoD network intrusions fell 46% after it banned passwords for log-on and instead mandated use of the CAC with PKI.

But Barriers Exist

• High assurance credentials come with higher costs and burdens
• They’ve been impractical for many organizations, and most single-use applications.
• Metcalfe’s Law applies – but there are barriers (standards, liability, usability) today that the market has struggled to overcome.
Barriers help guide where Pilots, R&D are needed

**Privacy**
- Privacy Enhancing Technologies (PETs) (i.e., zero knowledge proofs)
- Model Frameworks for Privacy Protection
- Business models to demonstrate viability of PET

**Usability**
- Are there ID solutions that can automate authentication and simplify the user experience?
- Can mobile solutions overcome challenges with tokens?
- Presenting choice in a way that does not overwhelm

**Security**
- Alternatives that can deliver the PKI model or something similar with “lighter weight” technologies
- Analysis of weak links in commonly embraced identity and credentialing schemes

**Liability**
- Model frameworks for Liability Allocation
- Innovative ways technology might be able to mitigate liability risks

**Interoperability**
- Lack of solid standards to enable interoperability between different credential platforms
- Architectures to enable easy exchange of identity and credential information
- Attribute exchange and linkage to credentials
Questions?

Jeremy Grant

jgrant@nist.gov
202.482.3050