



Bringing Trust to Applications with Hardware-Based security

Rick Doten

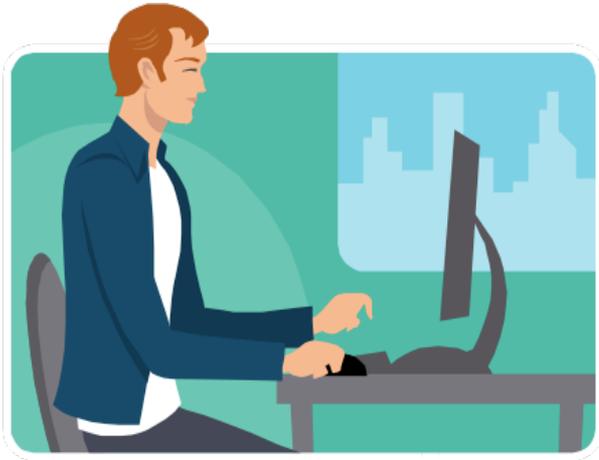
CISO

DMI

September 19, 2012

A typical day at work for Ray:

Ray works for a company with a mature security architecture and uses all best practices



- › Ray logs into his system, brings up email, and goes through messages
- › He sees a email from a trusted partner and opens the attachment
- › Ray finishes mail and logs into an internal web-based workflow application to check progress of a proprietary project being worked
- › He then goes to Internet and logs into brokerage account to check stocks; he uses personal token for strong authentication.
- › Ray checks his email again, cause he can't help it
- › Ray brings up customer's sensitive application that requires him to plug in his ID card into reader for authentication

What Happened During Ray's Typical Day?

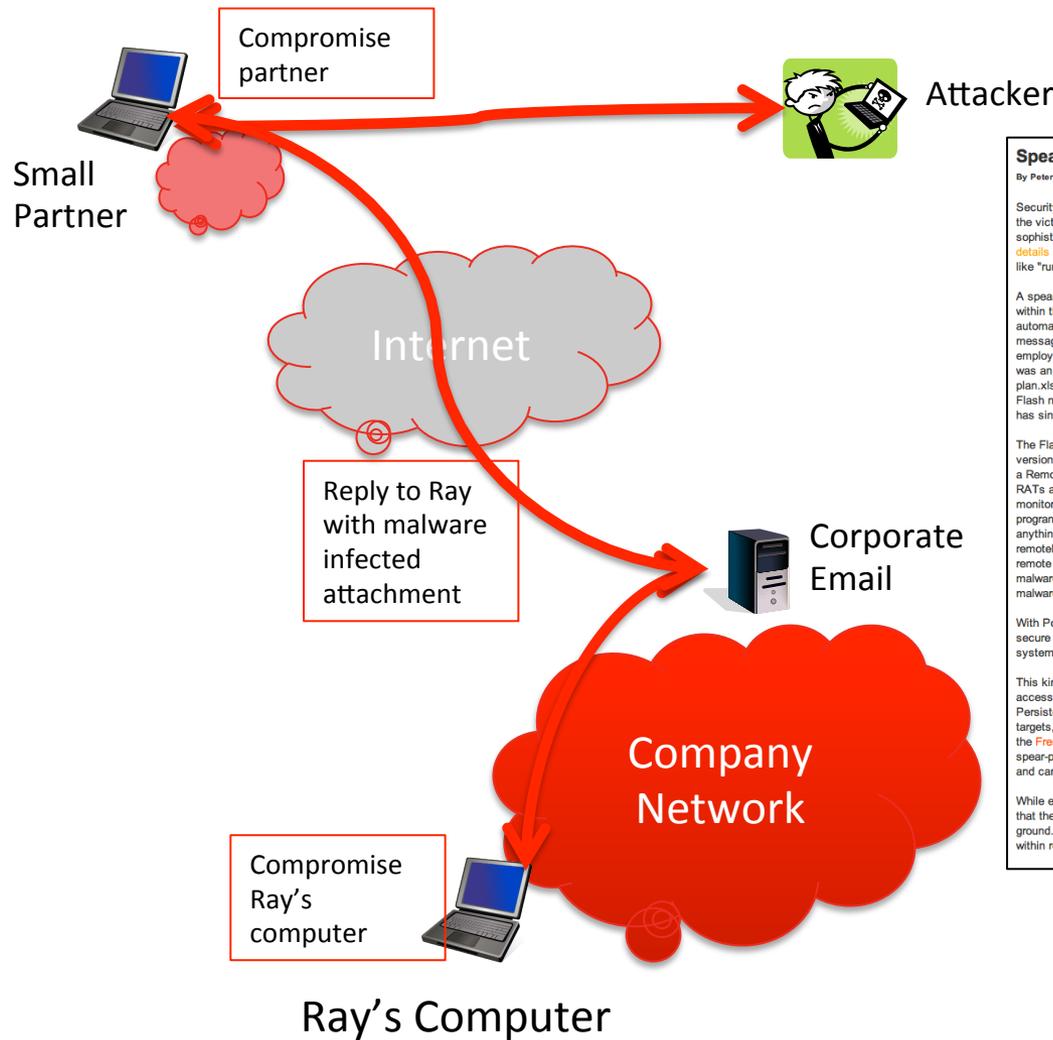
An attacker stole the credentials without Ray ever knowing for:

Rays Corporate account, Personal Account, and Customer Account.



How did they do it?

What Really Happened? Day 0



Spearphishing + zero-day: RSA hack not "extremely sophisticated"

By Peter Bright | Published 10 months ago

Security firm RSA **announced** in March that it had been the victim of a hack that it described as "extremely sophisticated." The company has now **shared some details** of the attack. "Extremely sophisticated"? More like "run-of-the-mill."

A spear-phishing e-mail was sent to two small groups within the company. Though the e-mail was automatically marked as Junk, the subject of the message ("2011 Recruitment Plan") tricked one employee into opening it anyway. Attached to the mail was an Excel spreadsheet, "2011 Recruitment plan.xls". Embedded within the spreadsheet was a Flash movie that exploited a Flash vulnerability. Adobe has since released an emergency patch for the flaw.

The Flash movie's payload in turn installed a modified version of *Poison Ivy*. Poison Ivy is known as a RAT, a Remote Administration/Access Tool/Toolkit/Trojan. RATs allow remote access to files, the registry, monitoring of network access, starting and stopping programs, and more, making them extremely powerful: anything the user can do locally, the hacker can do remotely. While in principle RATs can have legitimate remote administration uses, their widespread usage by malware and silent operation means that most anti-malware software will detect and remove them.

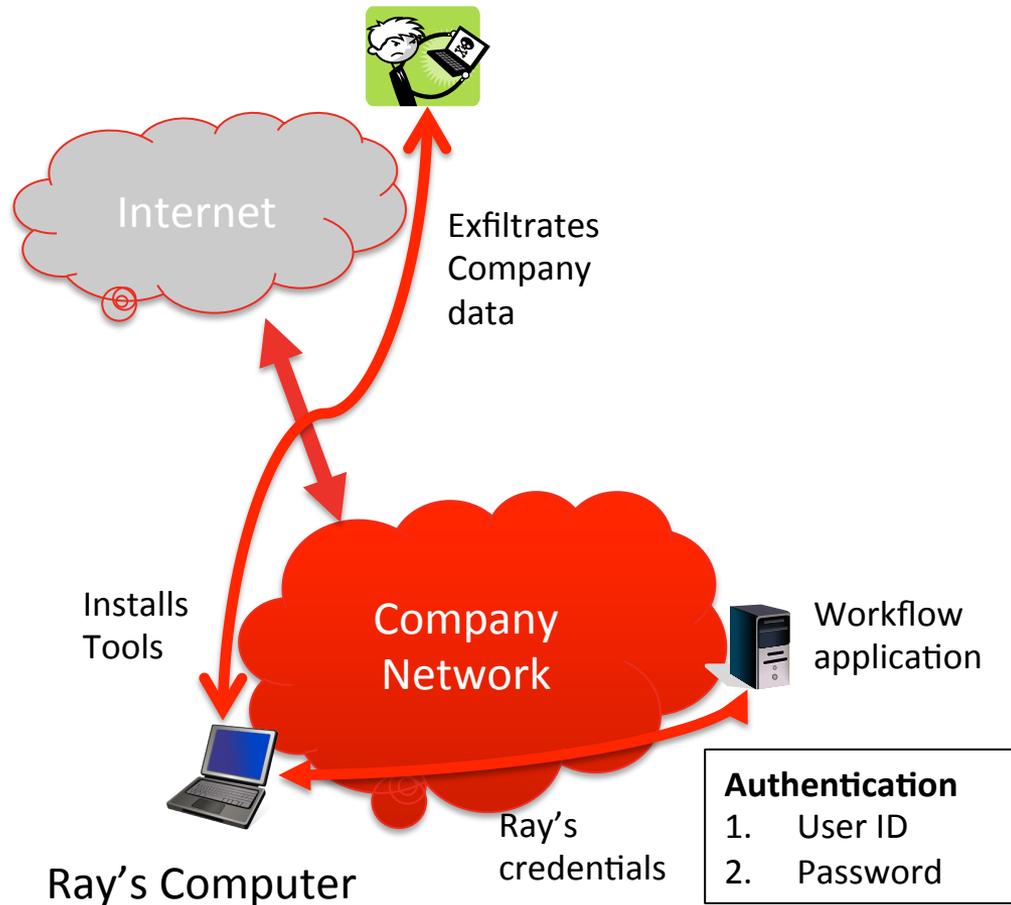
With Poison Ivy installed, the attacker stole user credentials and escalated their privileges to gain access to secure systems that the originally compromised user didn't have access to. The attacker then used this system access to exfiltrate some amount of sensitive data, the nature of which RSA is still yet to reveal.

This kind of attack, where an attacker deploys malware inside an organization that allows continued interactive access that allows them to react to what they learn about the target's environment, is called an Advanced Persistent Threat (APT). APTs represent a significant threat to high-profile organizations. Among other targets, APTs were used in the *Aurora attacks* against Google (and others), and also in the attacks against the *French* and *Canadian Finance Ministries* earlier this year. The attacks all tend to follow a similar pattern—spear-phishing with a zero-day exploit to penetrate the organization and deploy long-lived malware, then a slow and careful process of learning more about the target and getting access to more sensitive systems.

While effective, however, it's a little hard to justify RSA's claims of extreme sophistication. This is not to say that the attackers were chumps, but judging by what RSA has revealed so far, no part of this attack broke new ground. The same pattern is being repeated with some regularity, and the tools to perform such attacks are within reach of any enterprising hacker.

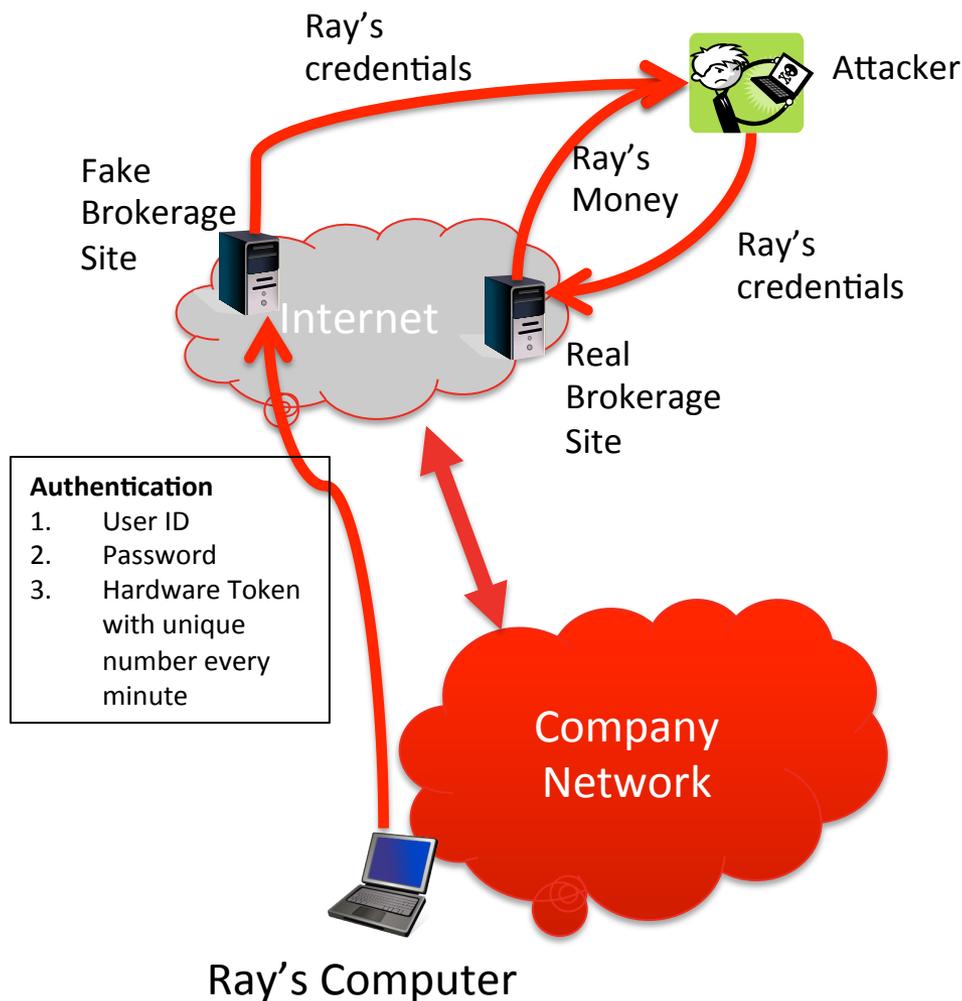


Day 1, Capture Account Credentials, Drop advanced capture tools



- The next day, the attacker uses captured credentials to log into the project workflow application with Ray's credentials and starts downloading documents.
- The attacker installs additional tools to allow him to get in the middle of the login, the next time Ray uses 2 factor authentication for more sensitive applications.

Day 2, Man in Middle secure application access, Brokerage account



- The following day, Ray logs into his computer, and performs almost the same routine as before; but things are different...



COMPUTING
Real-Time Hackers Foil Two-Factor Security
One-time passwords are vulnerable to new hacking techniques.
FRIDAY, SEPTEMBER 18, 2009 | BY ROBERT LEMOS

Audio »

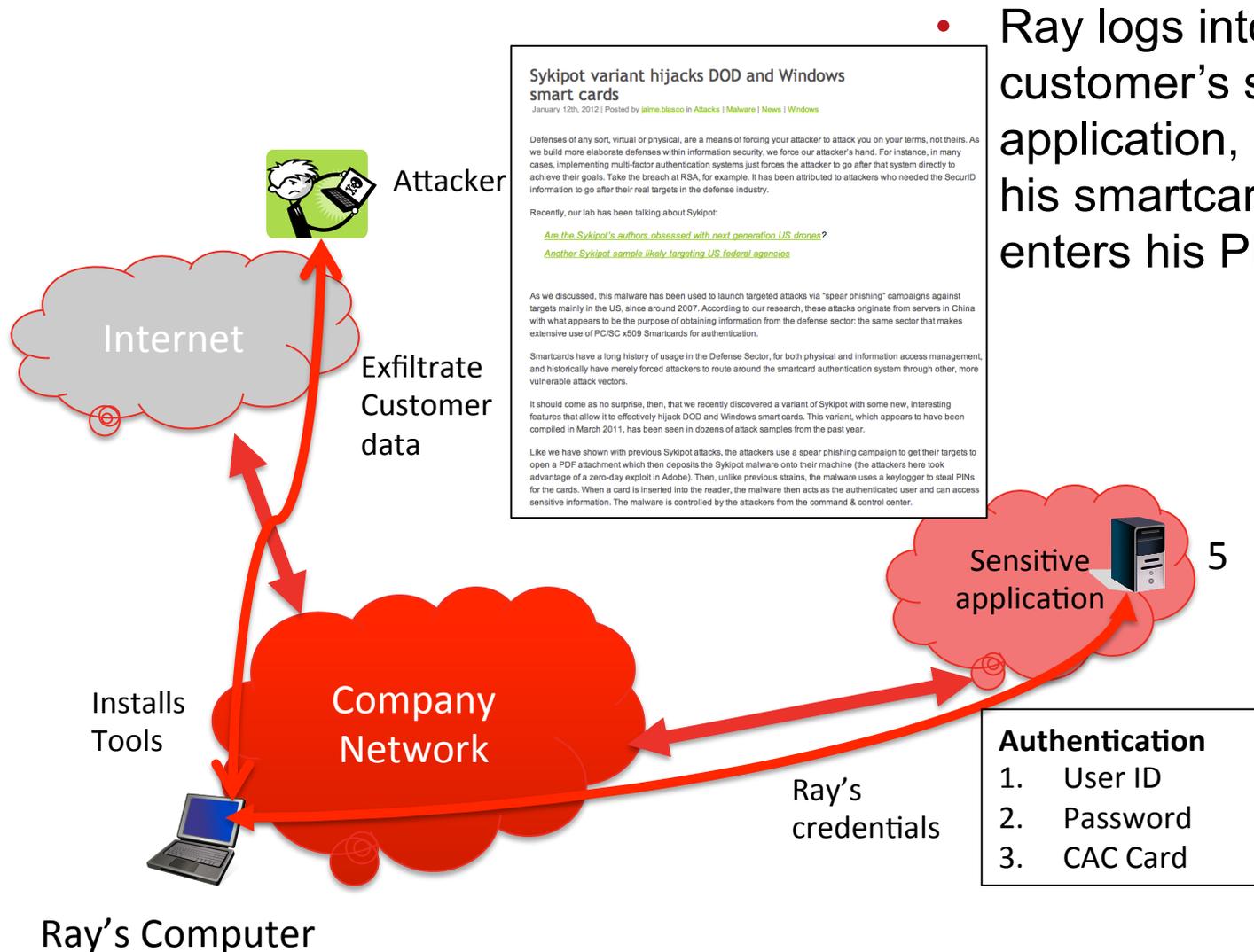
In mid-July, an account manager at Ferma, a construction firm in Mountain View, CA, logged in to the company's bank account to pay bills, using a one-time password to make the transactions more secure.

Yet the manager's computer had a hitchhiker. A forensic analysis performed later would reveal that an earlier visit to another website had allowed a malicious program to invade his computer. While the manager issued legitimate payments, the program initiated 27 transactions to various bank accounts, siphoning off \$447,000 in a matter of minutes. "They not only got into my system here, they were able to ascertain how much they could draw, so they drew the limit," says Roy Ferrari, Ferma's president.

The theft happened despite Ferma's use of a one-time password, a six-digit code issued by a small electronic device every 30 or 60 seconds. Online thieves have adapted to this additional security by creating special programs--real-time Trojan horses--that can issue transactions to a bank while the account holder is online, turning the one-time password into a weak link in the financial security chain. "I think it's a broken model," Ferrari says.

Security experts say that banks and consumers alike need to adapt--that banks should offer their account holders more security and consumers should take more steps to stay secure, especially protecting the computers they use for financial transactions.

Day 2, Man in Middle secure application access, Customer Application



- Ray logs into his customer's sensitive application, he inserts his smartcard, and enters his PIN.

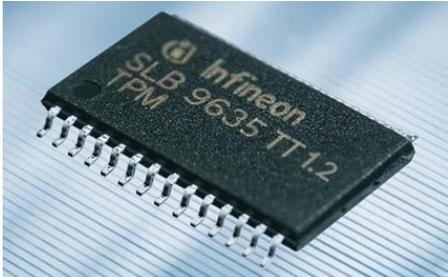
How Could this be prevented?

Two Technology Options:

- ◆ Credentials stored and protected in Trusted Processor Module (TPM)
- ◆ Trusted Container protected by hardware root of trust.



Trusted Processor Module (TPM) – How does it work?



TPM's provide a foundation of trust based on minimum set of security features:

- protected capabilities
- integrity measurement
- integrity reporting



These allow you to:

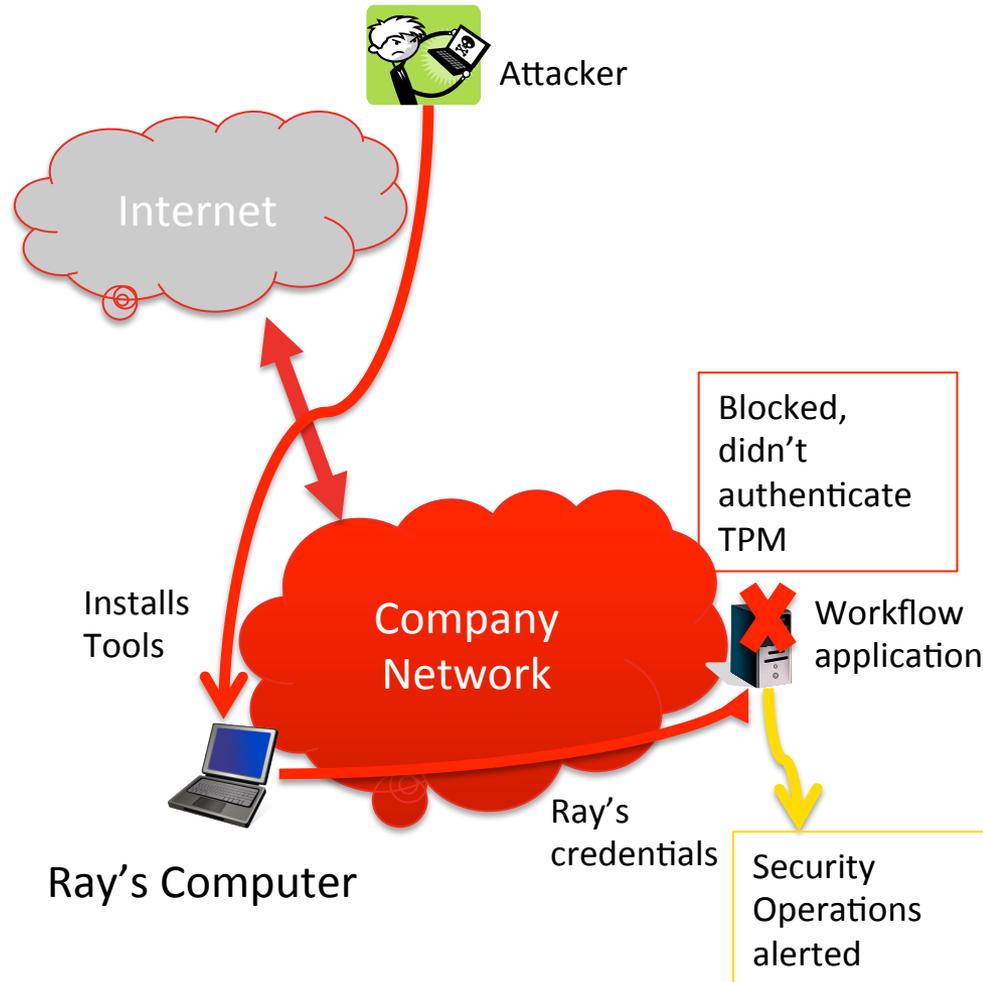
- Securely store cryptographic keys
- Perform Integrity checking on hardware components (i.e., BIOS, MBR)
- Perform attestation on processes
- Root of a chain of trust

How does this help applications?

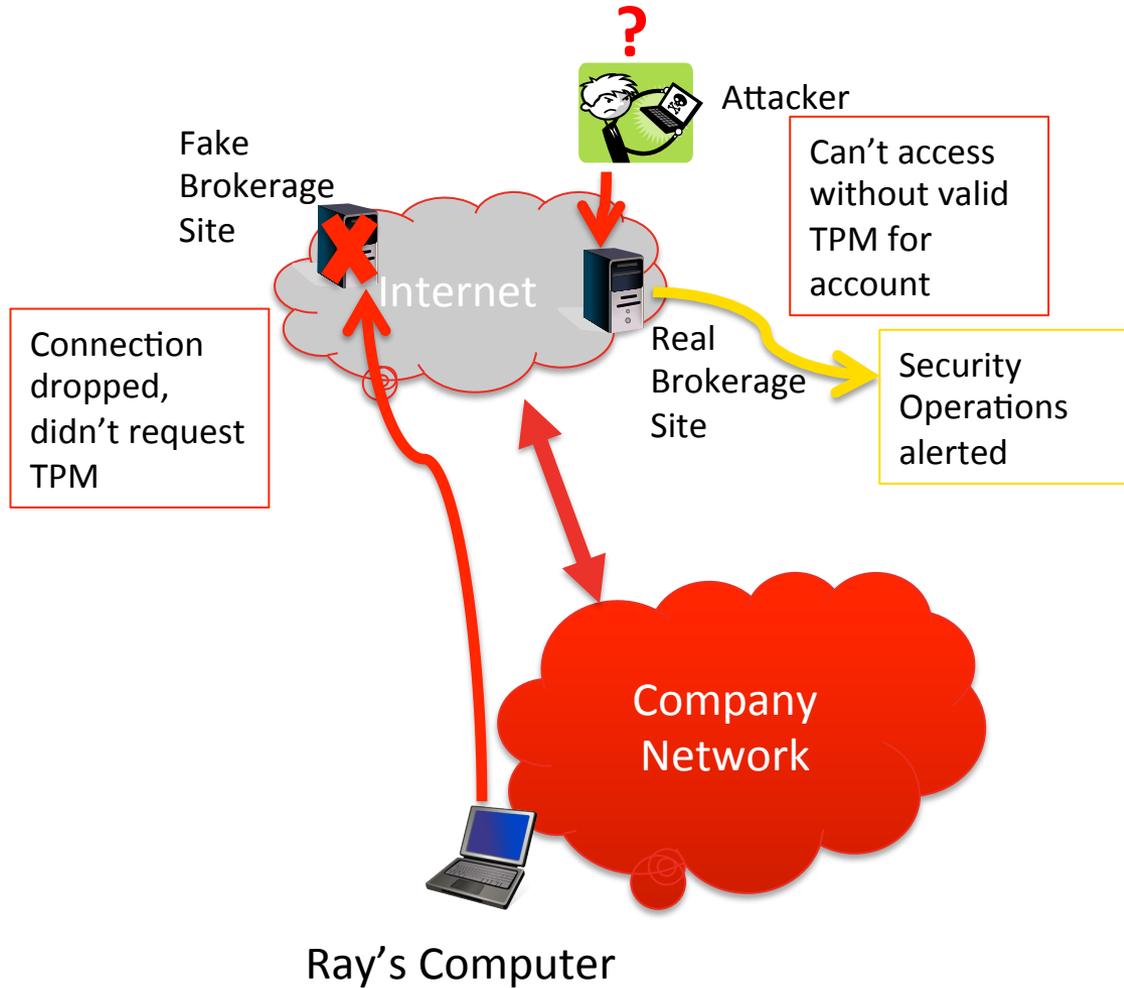
- Secure store of credential that cannot be spoofed, captured, or replayed
- Linking TPM to application authentication can prevent these specific attacks, and alert that there is a problem
- Requiring secure container for sensitive applications will prevent corrupted systems from accessing application

-

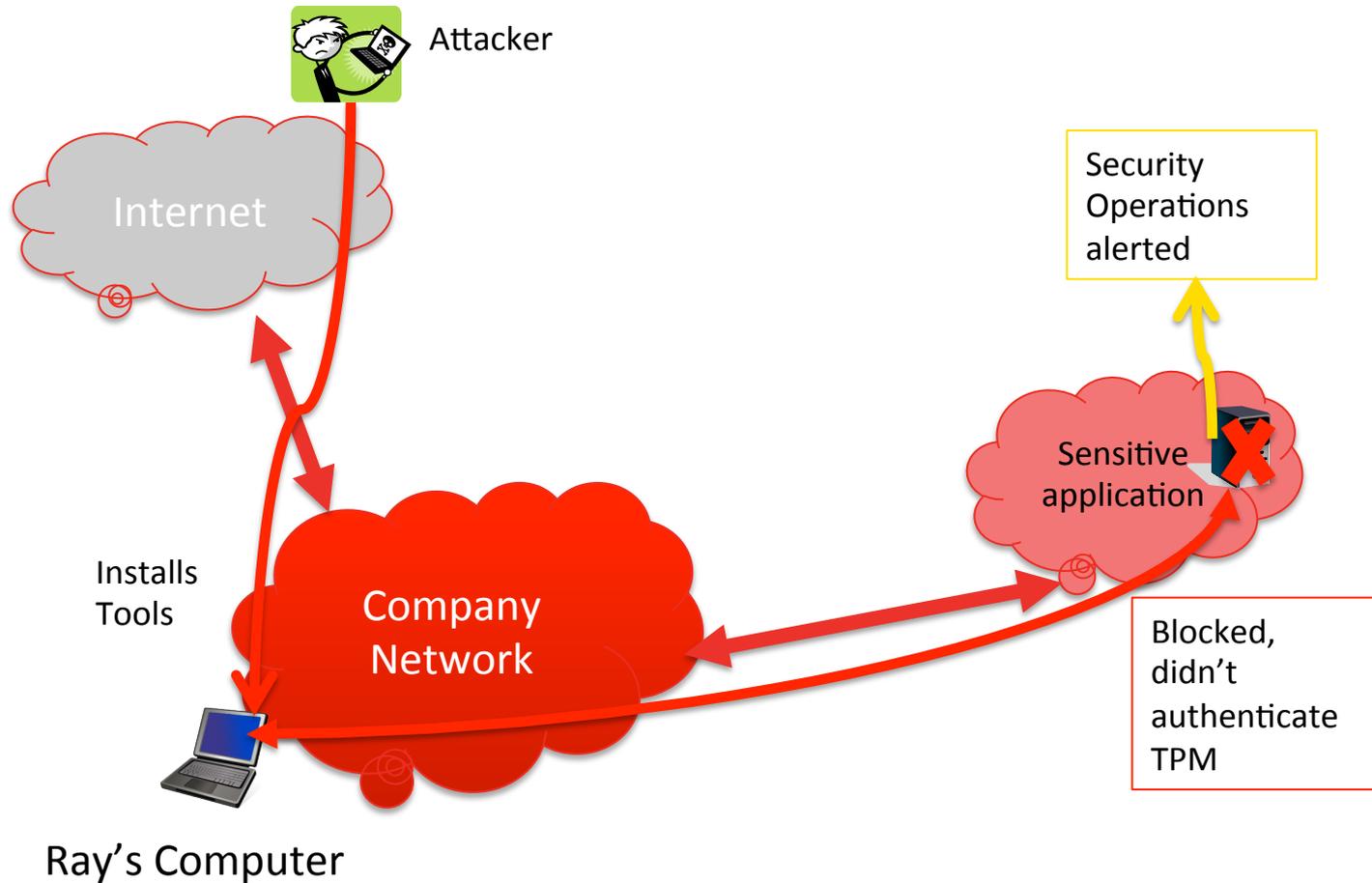
Ray's company Workflow application could be protected by TPM authentication



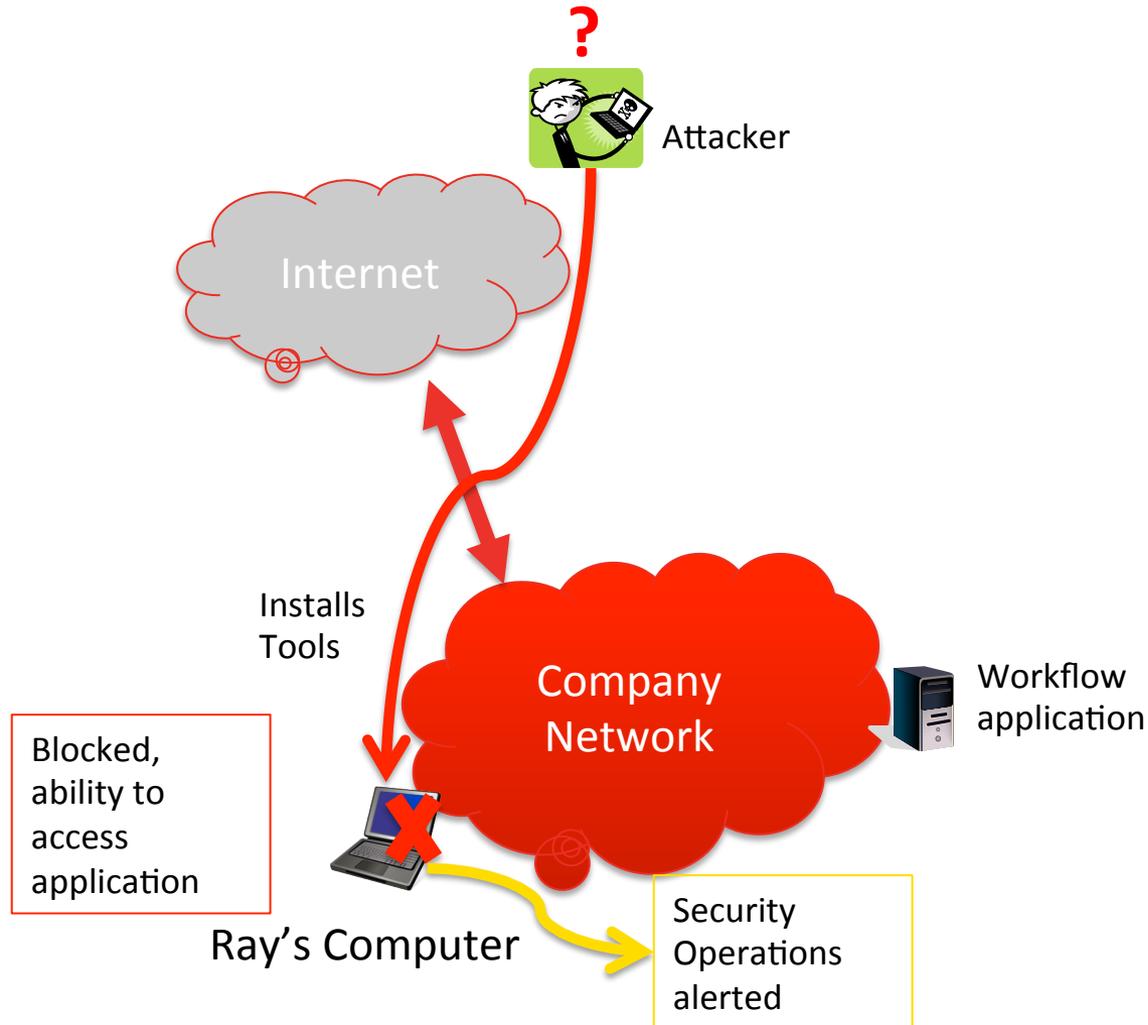
How Ray's Broker could protect him with TPM authentication



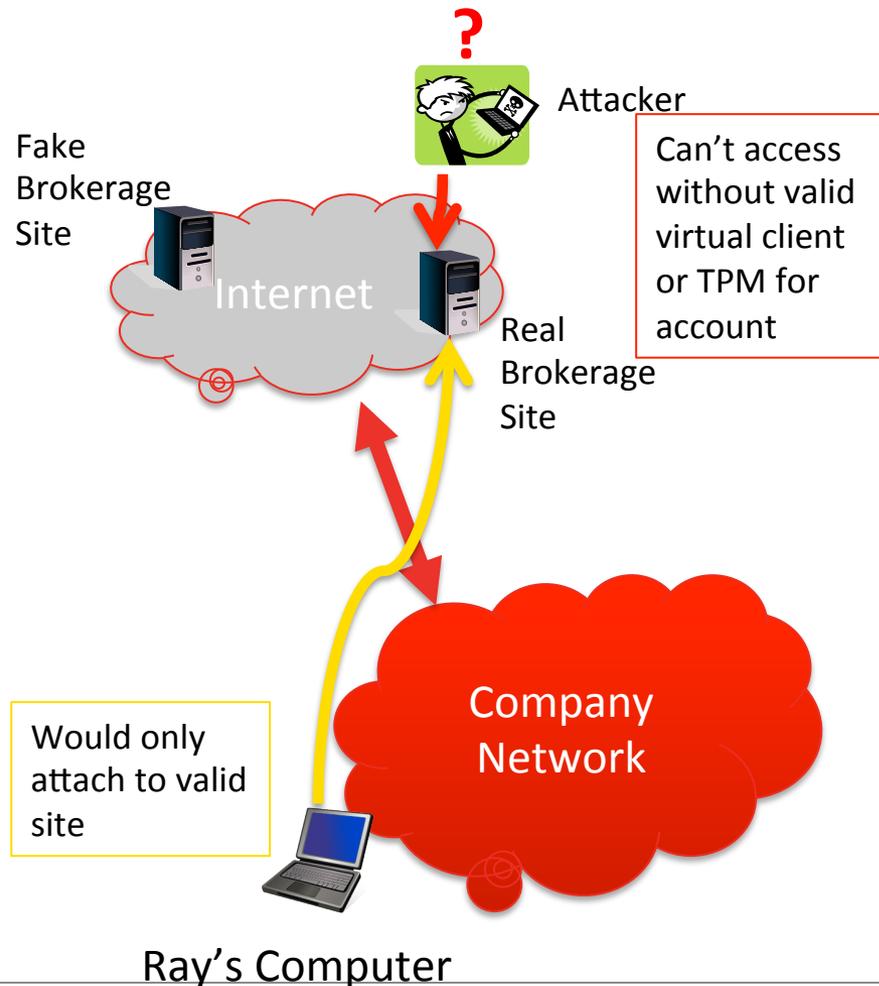
Ray's Customer Application could be protected using TPM



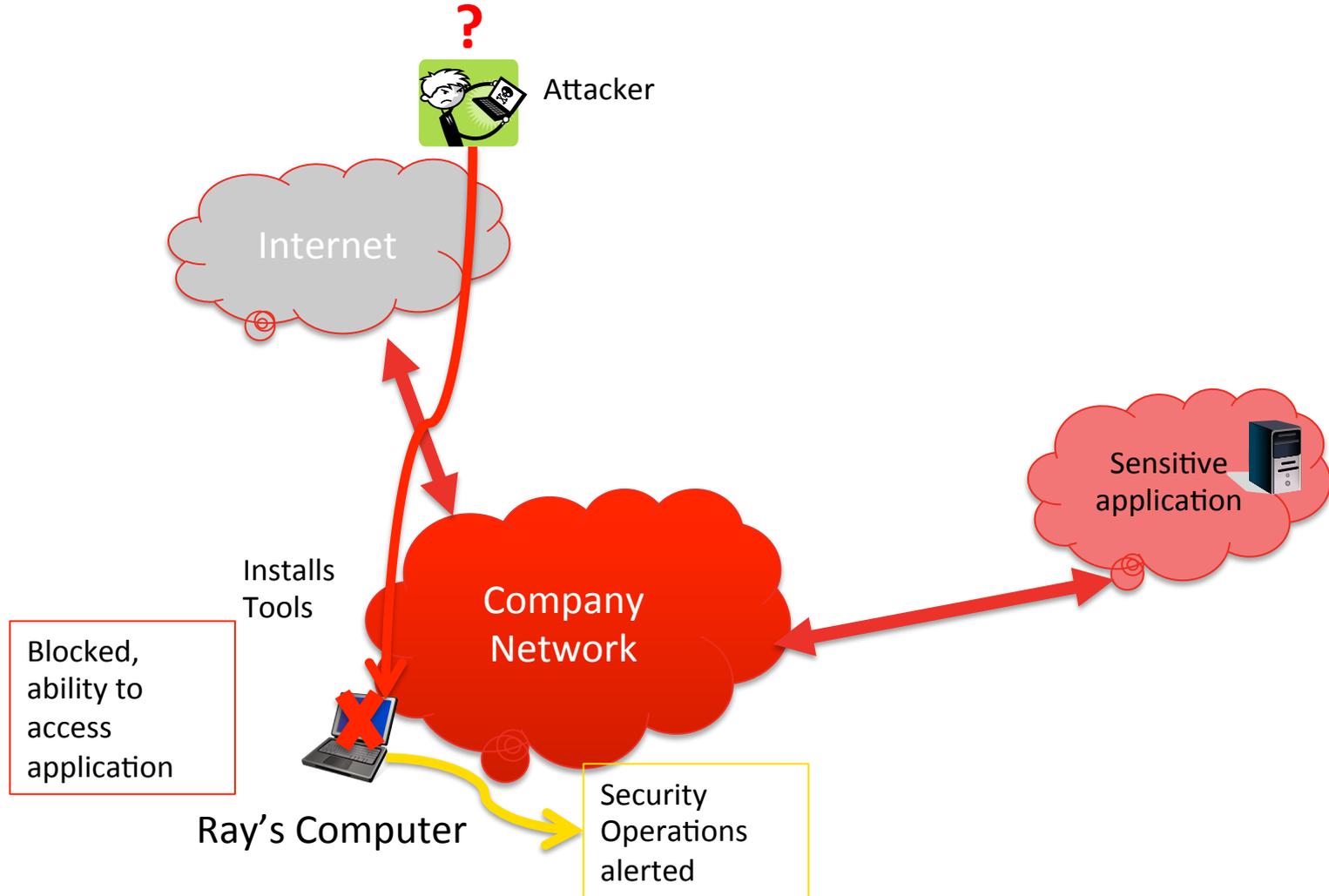
How Ray's Workflow Application could be protected with Trusted Container



How Ray's Broker could be protect with Trusted Container



Ray's Customer Application could be protected using Trusted Container



Future Applications for Trusted Technology



- **Trusted Online Transactions**

- › Strong trusted authentication for all transactions
 - Credentials that cannot be captured or spoofed; phishing sites and keystroke logging would be a thing of the past allowing:
 - › E-Commerce
 - › E-Voting



- **Environmentally Conscious**

- › With trusted electronic signatures, huge stacks of paper being printed for legal and real estate transactions will be a thing of the past.



- **Privacy Control**

- › Privacy through encryption of data at rest and in transit, and the ability for granular access control

Questions and Discussion





Thank You!

Rick Doten, CISSP, RKC
Chief Information Security Officer
DMI
Bethesda, Maryland
rdoten@dminc.com