Implementing HIPAA Security – A Real Life Experience

March 15, 2002
HIPAA Summit West II
San Francisco, California

Computer Sciences Corporation
Healthcare Group
1325 Avenue of the Americas, 6th floor
New York, New York 10019
Phone: +1.212.401.6000
Fax: +1.212.401.6800

Agenda

I. The Setup

II. The Players (Anonymized!)

III. Security Tasks

IV. Mission Creep

V. Conclusion

The Setup

The Client – a Health Care Clearinghouse

- Small, but backed by major payers
- In need of System Integration
- Core Payer Security Requirements:
    - HIPAA Compliant
    - Public Key Infrastructure

Our initial security tasking was limited to the PKI

The Players

Computer Sciences Corporation

Computer Sciences Corporation, one of the world's leading information technology services providers, helps organizations achieve business results through the adroit use of technology. CSC is currently a 10.5 billion dollar, 68,000 person company. No other company offers the same range of professional services and global reach as CSC does in areas such as security, e-business strategies and technologies, management consulting, information systems consulting and integration, application software, and IT and business process outsourcing.

Payers

- Several of the largest insurance companies in the United States backed the clearinghouse
- They have a vested interest in ensuring the success AND security of the arrangement
- As industry powerhouses, they are used to calling the shots – the 800 lb. gorillas defer to them

The Clearinghouse

- Initially consisted of a few executives and a CSC-led team of technical/business personnel
- Starting from scratch – the Clearinghouse had a custom designed application to receive claims status, eligibility requests from providers; reformat and send request to payer; send answer back to provider in real time
- Marching orders in security based on a previous consultant’s recommendations.

Security Tasks

Selecting the Vendor

- There are several vendors of PKI packages. We wanted a package that was
  - **Turn-key** – given the time frame, we needed plug-n-play
  - **Cost effective** – as always
  - **Scalable** – the pilot was to be limited, production to be large
  - **Disposable** – if the pilot didn’t work, we wanted the loss to be bearable

- We settled on VeriSign OnSite because
  - **It met all the factors above, especially Turn-key**

Factors

Feature	Pilot Needs	OnSite
# of users	200-500	Minimum of 500
Cost	Cost control desired	$45,000
HIPAA Compliant	Not required for pilot. However, HIPAA compliance required for production roll-out	Yes – root certificate formally documented
User Authentication	Providers authenticated prior to pilot in selection phase	Choice of automatic, manual, or outsourced to VeriSign
Reusability in production phase	Dependant on cost	Yes
Users may keep the same certificate after the pilot	Desirable, but not required	Yes – the root CA would remain the same
Prevent users from exporting certificates to other machines	No requirement defined	Yes
Single logon	No requirement defined	Yes (with integration)
Roaming capability	No requirement defined	Yes
Scalability	None	Yes

We made the selection, let’s get it done

- Installation went smoothly
- We opted to use manual authentication for the pilot
  - Automatic authentication required a pre-existing database of authorized users; not available at this stage of the game
- Time to install certificates on user desktops
  - Our first snag!

The Users

Users = Providers

- On a practical level, most users were nurses and office workers
- Most were not computer savvy
- We sent people to individual provider offices to help them register for certificates
  - A significant percentage still had problems
- Result – lots of time on the phone for the PKI Admin

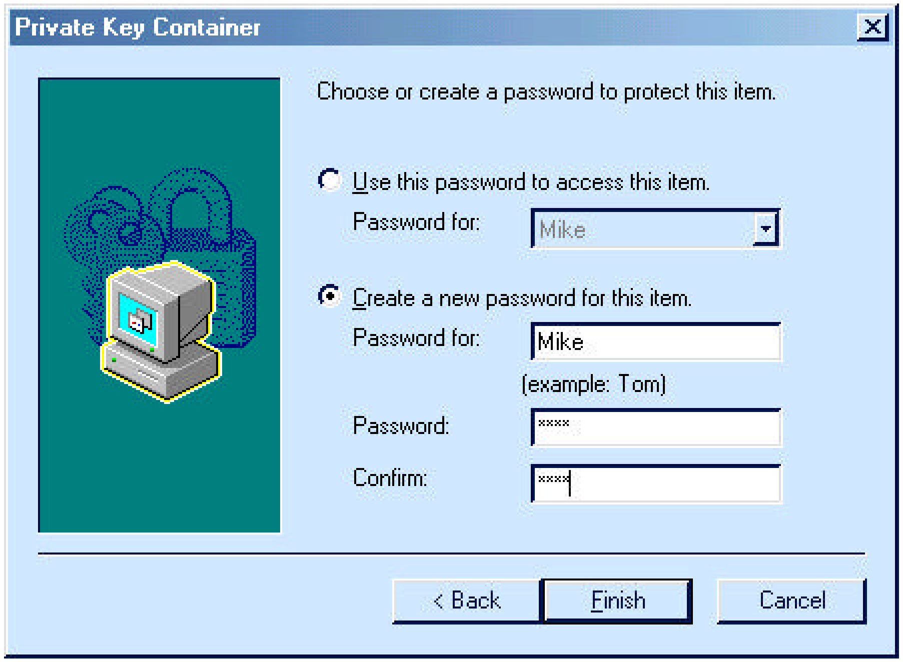
Our Main Interest was a Functioning PKI

- We did not plan on using the certificates for Role-based Access Control
  - This was built into the custom application
- The sole use (for the pilot) was authentication
  - This was for simplicity
  - If the authentication features were functioning, so would add on features (encryption, digital signatures, etc.)
- There were plans for additional capabilities in the future

The First Usability Problem

OnSite’s Manual Administration Mode

- The full version of Onsite with all the bells and whistles includes a plug-in called GoSecure
- While considered an “option”, it really isn’t
- It replaces the crypto modules in Internet Explorer
- A problem may arise:



Private Key Container

Choose or create a password to protect this item.

○ Use this password to access this item.

Password for: Mike

● Create a new password for this item.

Password for: Mike

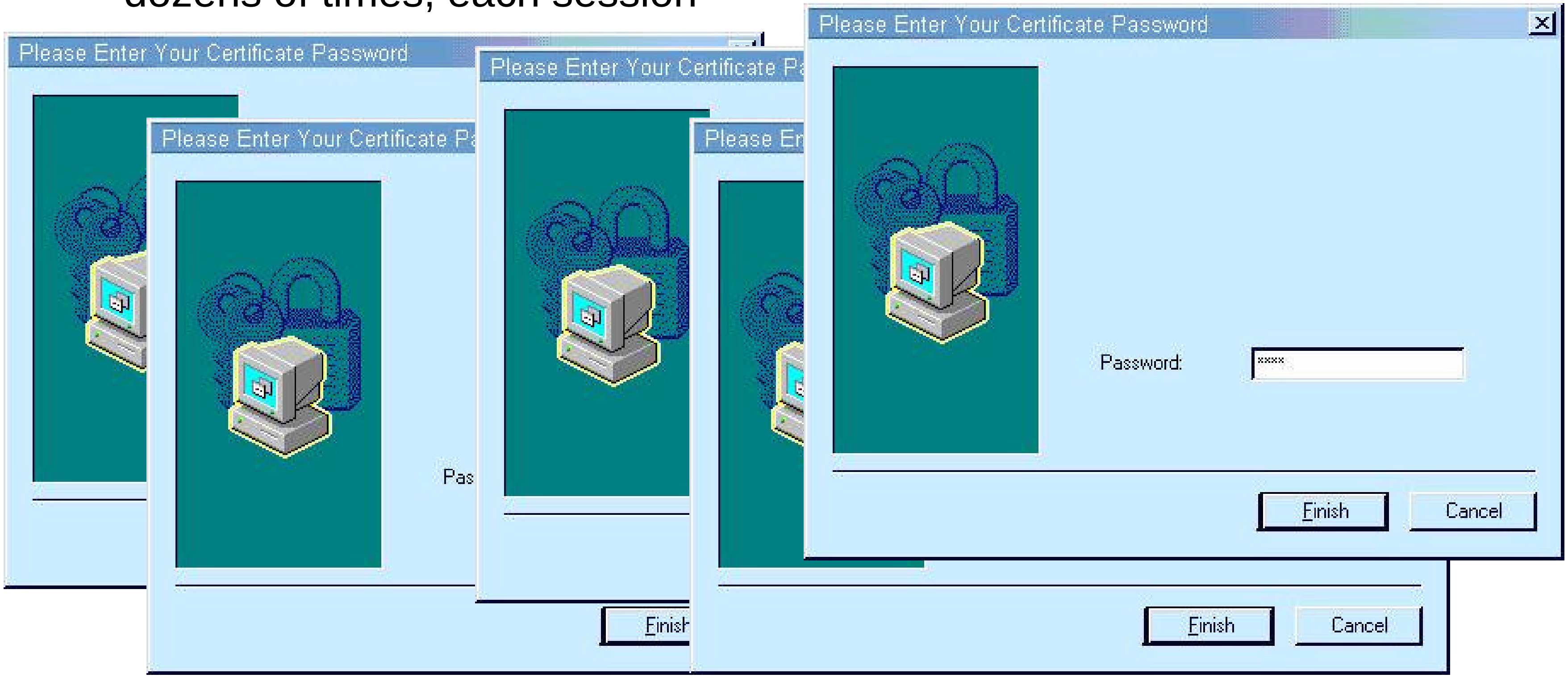
(example: Tom)

Password: ****

Confirm: ****

Choose High Security, Choose Major Irritation

- An undocumented “feature” found in Windows 9x and Windows NT is that the password popup window will show and require a password each time the key is accessed within a single session – potentially dozens of times, each session



Please Enter Your Certificate Password

Password: ****

And We Fixed It!

- Microsoft explained that this was a design feature of Win9x and NT, and that it had been fixed in WinMe and 2K
  - This behavior you describe is actually by design. When the feature to password encrypt the certificate locally was implemented, it was done so that each request would require the password to be retyped. In Windows 2000 the implementation was changed. The reason it is saved in Windows 2000 is because subsequent calls (calls after the first request for the cert password) to CryptSignHash use a cached private key in Windows 2000 and does not in the down-level clients.Your only options are to disable the "strong private key encryption" or upgrade the clients to Windows 2000
- Another solution would have been to ditch IE and use Netscape, which did not suffer from this “feature”
- Neither was practical

And the Complaints Rolled In……

The clearinghouse depended on convenience to sell the product

- Multiple password entries are clearly not convenient
- The PKI *did* work for authentication
  - It was just a pain in the stethoscope
  - We had demonstrated the concept
  - We knew the cure
- Declare Victory and Depart
- We shut down the pilot

We Worked to Make the Production Rollout an Unqualified Success

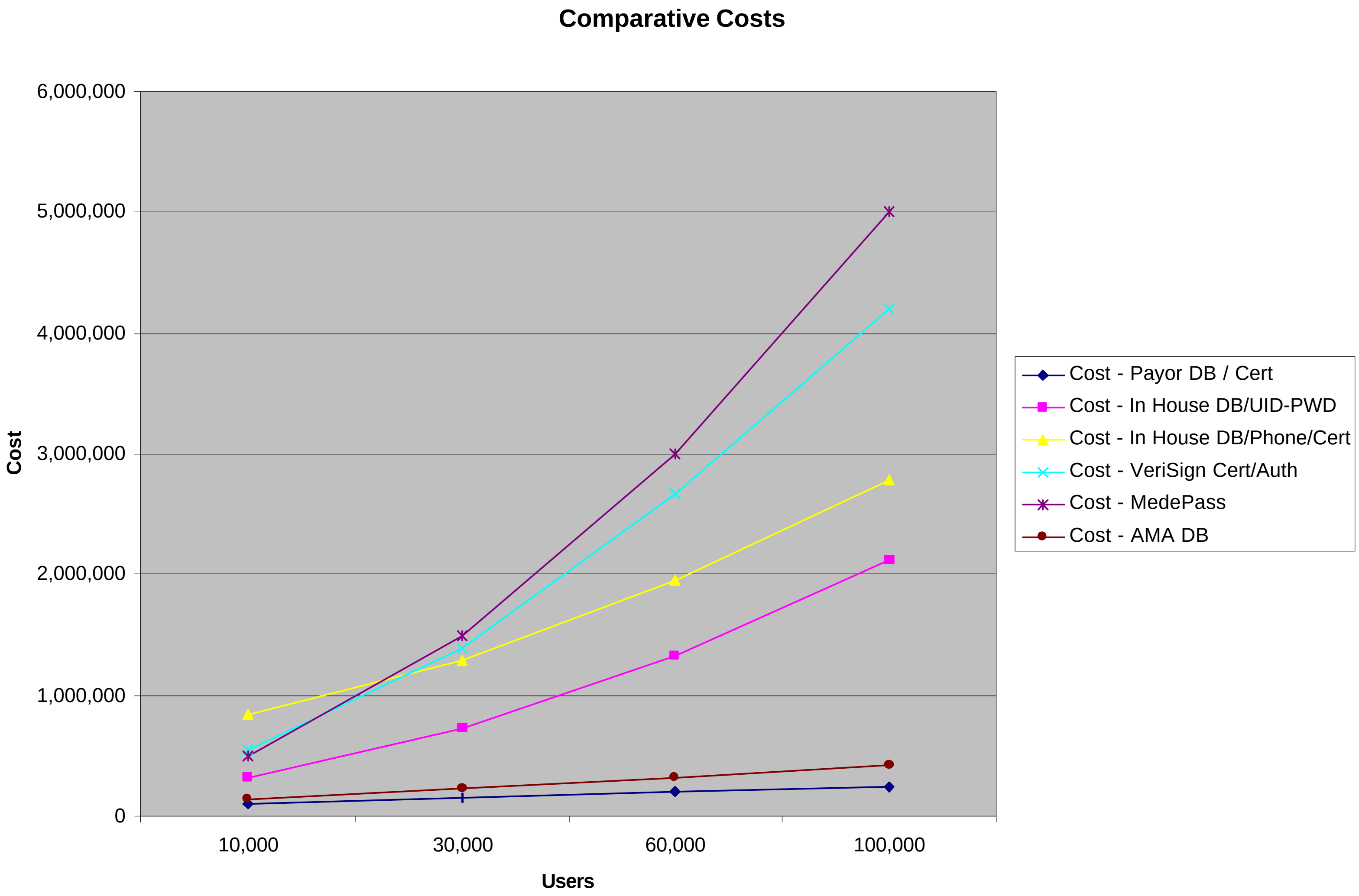
- Planned the procedures and LDAP needed for automated authentication
- Developed policies to cover authentication requirements
- Other security issues came to the forefront
  - Negotiations with those payers
- In general, the payers advocated the platinum security solution, while the clearinghouse favored the economy family-size solution
- This did not contribute to harmonious talks

Let’s Look at Longer Term PKI Dollars

- We were crunching numbers using estimates supplied to us by VeriSign, others…
- The costs were looking staggering…

Meanwhile……

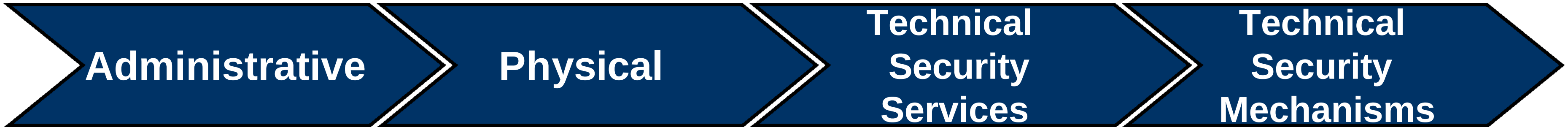
Various Options versus Costs



Final PKI Decision

HIPAA is Much More Than PKI

In Fact, HIPAA Doesn’t Require a PKI



Administrative

Physical

Technical Security Services

Technical Security Mechanisms

- Policies and Procedures

- Locks, Storage, Physical Access Control

- Auditing, Access Control, Authorization, Authentication

- Network Security

Those Discussions With the Payers Were Still Ongoing

The Clearinghouse used Payer patient data

Administrative

- **Policies and Procedures**

Privacy

- **Use, Disclosure, Chain of Trust**

•No one at the Clearinghouse ever accessed the patient data

•Nonetheless, the data was flowing from the Payer to the Clearinghouse and the Payers needed assurance that the data was secure

•Therefore, a Chain of Trust Agreement had to be negotiated between all parties

•Closest analogy: "Herding Cats"

Mission Creep

Build a PKI – but there's more than that in HIPAA

- There's more to HIPAA than just the issues addressed by a PKI
- One of the 4 security areas – Administrative Measures – is commonly neglected and usually not sufficient for HIPAA even in conscientious organizations
- Policies and Procedures must be defined in substantial detail AND enforced
- We became policy writers as well as technology integrators

HIPAA Security Rules define 12 areas that must be covered

- These are not necessarily exhaustive – more policies might be needed for some organizations
- Step 1: What policies already exist at the Clearinghouse?
  - **Answer – not many**
- Step 2: What policies will we write?
  - **A full policy writing effort for an organization of this size and complexity would probably take around 3 months of full time effort**
  - **Well beyond the scope of work**

Technical Security Mechanisms

- HIPAA requirement for alarms, audit capability on the network
- This capacity did not exist
  - **Interim answer – Snort**
- Capable, open source IDS
- Installed at the hosting center
- Also wrote Incident Response policy/procedure based on public documents and Clearinghouse needs
- As Production neared, we developed an IDS architecture using a commercial system

The Clearinghouse gained capabilities by acquiring another company

- How secure is the other company? Go out and look at it
- How do we integrate their infrastructure with ours?
- How do we achieve Single Sign-On?

Conclusion

HIPAA Security is a multi-headed beast

- PKI is most appropriate when your users are already well known to you
- The cost of authenticating users can be huge
- The cost of certificates can also reach the stratosphere
- All four HIPAA security areas must be addressed in parallel
- Getting multiple parties to agree to a single security policy is a long process; multiply that by the number of policies to be written
- The deeper you look into some of the requirements (especially auditing access), the more daunting they can seem

Conclusion

Ultimately our security effort was successful

- We built a secure authentication infrastructure
- We wrote a number of important policies
- We built an interim Intrusion Detection System
- We helped to integrate two companies’ infrastructure