# It's All About Authentication -- Again!

Jeffrey I. Schiller
MIT

# A Quick History of Network Computing

1970's -- Only researchers on the network

1980's -- Students too

And so it begins...

1980's: Our Network is protected by the fact that all of the data going over it is boring... very boring.

**But:** Passwords are Interesting

One of the key motivations behind the development of *Kerberos*

# Passwords Smashwords...

1990's: Password stealing attacks begin

Frankly, we were surprised it took so long

1990's: Networking Goes Mainstream, PC's at home. Targets galore!

*And they were all based on a toy operating system, exploits abound.*

The age of Virii. No Memory Protection, unsophisticated users. Target Rich Environment.

# The Decline of Password Stealing

Worms, Viruses, Trojan Horses, Buffer Over-runs. Who needs to steal passwords...

Passwords better protected. Many sent over SSL (https) or "ssh" (one of the most influential network tools for all time!) [OK, SSL is important too...]

But the fire smolders...

# Smoldering...

Password Quality Suffers, Some websites insist on "strong" passwords. So... people pick a "strong" password (or not) and use it everywhere.

So who owns a password?

As a system administrator, you may think you own your users passwords

# But you Don't

If they can change it. If they can share it, if they can use it elsewhere, they own it. I don't care what fantasy you believe!

And now they are targets. Sure we have Viruses, Worms and Trojans... AND THEY STEAL PASSWORDS!

*And all the network encryption doesn't help us here....*

# Why?

Do I really have to say? If you own someone's password(s), you own them.

Of course not everyone is as valuable.

People who control money, or important infrastructure are serious targets. Look what happened with EDUCAUSE

# So what do we do?

Hello? Where have you been?

Smart Cards? -- Been there, tried that. FAIL

USB Tokens -- Ditto (no thanks to the iPad which doesn't have a USB port)

The only technology that has gained any (and it isn't much) traction are one-time password tokens. The kind that give you a six digit code to type in yourself.

# Why are they winning?

No hardware required [readers] (Multics failed because it required specialized hardware... and we didn't learn the lesson)!

No Hardware required [tokens]. "Soft" tokens can be installed on phones. SMS messages can be sent with codes. Heck you can even write them down on paper or have them voiced to you on a POTS line.

# People Still Hate Them...

People want passwords... just like they want dancing Bears.

Show me a layman who likes two-factor tokens and I'll show you a victim of identity theft. Remember Matt Honan.

Which bring us to...

# Human Factors -- Password Resets

The next frontier will be the helpdesk. If you cannot steal a password (or its worthless because it is one time), then you attack to support organization. "Hey I forgot my token, can you issue me a new one."

Or

Hi Phone Carrier, This is [Important Person], I just got a new cell phone. Its IMEI number is...

# From the other side

I have [Important CEO] on the line. If I don't do what he says and it is really him. BAD BAD

If it isn't him and I do it, will I get blamed (probably not).

Three guesses what happens here.

# What to do

Differentiate your user population into people with awesome powers and people without (you can define "awesome powers").

Help Desk can only reset credentials for "normal" people. People with awesome powers have to be handled by someone more seniority (someone who can say "no" to the awesomeness).

# Btw -- Awesomeness

It isn't about political power. It's about ability to do harm. One of the most awesome people at your institution is the one who can login to your domain name registrar and redirect your DNS servers.

(we know this real well at MIT!)