Introduction to Computer Security
Revision Notes

James Brown

April 21, 2017

Contents

1 Introduction

2 Usability and Security

Balancing security and usability is important - often it may be cheaper to simply pay to fix the damage caused by a security breach rather than simply paying for security needed to stop the breach. Breaking SSL - use a man in the middle attack. Users may just ignore the certificate warning. More than 80% of people in some browsers just accept the fake certificate on high-risk website (such as banks), allowing simple man in the middle attacks. In low risk situations, users proceed in about 100% of cases!

2.1 Social Engineering

Often computer security experts overlook non-technical attacks. Shoulder surfing is simply reading data from someone's screen from behind or while they aren't looking. It's also possible to get information by dumpster diving - from paper documents that may have been thrown away for example. These attacks are remarkably hard to stop

In general people want to be helpful - why not just phone them up and ask for: passwords, credit card numbers etc. Another possibility is an attacker may say they have come from the phone company and just walk straight into your server room. In cases where people are smartly dressed, a lot of the time we are more likely to trust them.

Often this leads to security experts thinking 'Users are stupid, they are the problem'. Bad security design is actually often the problem, users are doing what they need to do in order to get the job done.

When is a new security measure good? When it saves more than it costs. Benefits can be very hard to calculate, but we know a security is bad when costs are greater than the total loses. This is why users may choose to have an insecure system if it helps them get their job done.