Kurzfassung der Dissertation

Titel: **On Security in the Digital Office**
Autor: **Jens Müller**

In den 1980er-Jahren etablierte sich der Begriff des digitalen oder elektronischen Büros, um die radikale Veränderung unserer Arbeitswelt vom analogen hin zum digitalen Zeitalter zu beschreiben. Obwohl das digitale Büro heutzutage in den meisten Unternehmen, Organisationen und Behörden Realität ist, basiert es noch immer auf von Altlasten behafteten Protokollen und Datenformaten. Diese Arbeit stellt eine umfassende Analyse der IT-Sicherheits-Bausteine des digitalen Büros dar. Der Fokus liegt dabei auf den Bereichen E-Mail-Sicherheit, Dokumentensicherheit und Druckersicherheit. Es werden signifikante Designfehler in den angewandten Technologien demonstriert, welche auf die frühen 1980er (PostScript), 1990er (PJL, PDF, PGP, S/MIME), und 2000er-Jahre (ODF, OOXML) zurückgehen. Dabei sind diese Technologien keineswegs überholt, sondern gelten mittlerweile als etabliert, unverzichtbar und allgegenwärtig: PostScript und PJL Interpreter sind auf fast jedem Laserdrucker weltweit und auf vielen Linux-Systemen verfügbar. PDF ist das wohl meistgenutzte Dokumentenformat überhaupt. PGP und S/MIME sind die wichtigsten Verfahren für Ende-zu-Ende E-Mail-Verschlüsselung und digitale Signaturen. OOXML und ODF, wie von Microsoft Office and LibreOffice genutzt, sind de facto Standard-formate für Textverarbeitung, Tabellenkalkulation und Präsentationen.
Ziel dieser Dissertation ist es, einen Beitrag zur IT-Sicherheit im digitalen Büro – einer Grundvoraussetzung der Digitalisierung – zu leisten. Gezeigte Angriffe sowie Gegenmaßnahmen beziehen sich dabei auf typische Arbeitsabläufe: Versenden von vertraulichen E-Mails, Arbeit mit Dokumenten, sowie deren Ausdruck auf Papier.

E-Mail-Sicherheit. Es werden praktische Angriffe auf Ende-zu-Ende verschlüsselte E-Mails demonstriert: Efail Direct Exfiltration, Convert Content Angriffe, sowie Sicherheitslücken die auf legitimen E-Mail-Features basieren. Diese Schwachsellen erlauben es einem Angreifer, an den Klartext von PGP oder S/MIME verschlüsselten Nachrichten zu gelangen. Darüber hinaus werden Angriffe zum Fälschen von PGP und S/MIME Signaturen in allen relevanten E-Mail-Programmen veranschaulicht.

Dokumentensicherheit. Basierend auf Standard-Datenformaten wie ODF, OOXML, PDF und PostScript werden die Möglichkeiten bösartiger Dokumente systematisch analysiert und verschiedene Spezifikations-Schwachstellen offenbart. Gefundene Angriffe reichen von einfachen Denial-of-Service Attacken, hervorgerufen durch bösartige Dokumente, über den Zugriff auf lokale Dateien bis hin zur Ausführung von beliebigem Code. Außerdem werden Schwächen bei PDF-Verschlüsselung aufgezeigt, die es erlauben an den Klartextes verschlüsselter Dokumente zu gelangen.

Druckersicherheit. Drucker gelten auch heute noch in vielen Büros als unabdingbar. Sie haben sich zu komplexen IT-Systemen entwickelt, die Zugriff auf vertrauliche Informationen wie Druckjobs haben. Dies macht sie zu einem attraktiven Ziel für Angreifer. Basierend auf Standard-Druckersprachen wie PJL und PostScript wird eine umfangreiche Analyse von Angriffen auf Netzwerkdrucker durchgeführt.