基于电源线的电磁信息泄漏建模与实验分析

徐艳云, 黄伟庆*, 范伟, 张萌, 魏冬

中国科学院信息工程研究所, 北京 100093

* 通信作者. E-mail: huangweiqing@iie.ac.cn

收稿日期: 2015-06-24; 接受日期: 2015-07-24; 网络出版日期: 2015-09-17

中国科学院战略性先导科技专项 (批准号: XDA06010701) 资助项目

摘要 电磁信息泄漏问题给信息安全带来重大隐患, 对电磁信息泄漏的研究具有重要意义和价值. 针对用于计算机等信息设备的电源线电磁信息泄漏问题, 研究基于电源线的电磁信息泄漏原理, 建立了基于电源线的传导和辐射泄漏模型, 并对基于双电流探头的测试方法进行了理论分析, 最后通过实测数据对电源线电磁信息泄漏进行了验证分析.

关键词 信息安全 电磁安全 泄漏发射 电磁信息泄漏 传导泄漏 辐射泄漏

1 引言

20 世纪 50 年代初, 美国军方发现计算机系统杂散的电磁辐射会导致一部分重要的信息泄漏, 由此发展了信息技术设备的 TEMPEST 技术的研究, 其主要针对电子信息设备的信息泄漏进行研究. 60 年代, 英国开始组织信息电磁泄漏防护与侦收技术研究, 随后德国、加拿大等国相继投入研究. 由于涉及军事机密甚至国家安全, 信息电磁泄漏问题自提出之日起就成为美国政府严格保密的军事机密, 研究成果和技术细节不允许公开讨论, 直到 90 年代, 美国等国逐渐解密了一批 TEMPEST 文件, 泄漏电磁发射的研究才公之于世^[1~6], 近年来在电磁信息泄漏领域不断出现新的挑战, 如密码芯片、电力线电磁泄漏问题^[7~17]. 20 世纪 80 年代, 我国开始关注 TEMPEST 技术, 在泄漏发射及其防护机理、泄漏电磁发射信息接收和重构、微机系统电磁泄漏防护技术等方面取得了一定的成果^[18~29].

目前, 在基于电源线的电磁泄漏方面的研究相对较少, 而随着信息技术的飞速发展, 计算机网络信息系统在社会的各个方面发挥着越来越大的作用, 与此同时, 电磁信息泄漏问题给信息安全带来重大隐患和威胁, 特别是电源线的电磁泄漏易于被忽视, 因此研究电源线的电磁信息泄漏原理, 分析基于电源线的计算机视频信息泄漏具有重大意义和价值.

2 基于电源线电磁泄漏原理分析

本节将对基于电源线电磁泄漏进行原理分析, 建立电源线传导和辐射泄漏模型, 并对基于双电流探头的测试方法进行理论分析.

引用格式: 徐艳云, 黄伟庆, 范伟, 等. 基于电源线的电磁信息泄漏建模与实验分析. 中国科学: 信息科学, 2015, 45: 1341–1354, doi: 10.1360/N112014-00324

图 1 辐射泄漏

Figure 1 Radiation leakage

图 2 激励信号

Figure 2 Drive signal

2.1 泄漏源模型

基于电源线电磁泄漏可分为电源线传导泄漏和电源线辐射泄漏, 其辐射源为计算机等信息设备. 任何处于工作状态的电磁信息设备 (计算机、打印机、电话机等) 都存在着不同程度的电磁泄漏. 计算机是一个非常复杂的电子系统, 外来的电磁辐射、内部元件之间、分系统之间、各传送通道间的串扰对计算机及其数据信息所产生的干扰和破坏, 严重地影响着工作的稳定性、可靠性和安全性^[30]. 电磁辐射除了对信息产生电磁干扰外, 还会导致电磁信息的泄漏, 电子设备的杂散电磁能量通过导线或空间向外扩散, 如果这些泄漏中存在设备所处理的有用信息, 即构成了电磁信息泄漏.

计算机电磁信息泄漏包括辐射泄漏和传导泄漏. 辐射泄漏如图 1 所示, 电磁能量以电磁波的形式通过设备的外壳、各种孔缝、连线电缆等辐射出去, 并伴随着计算机系统各部件工作时的电磁辐射产生. 各种传输线、信息处理电路、时序电路、显示器、开关元件及接地系统等工作时起到天线的作用, 向外产生电磁辐射.

计算机中的并行信号为一个完整的信息在二进制转换下被分解成多位并行代码信号, 由多位并行线路同时传输或处理, 尽管可能产生辐射, 但由于这些并行线路相距很近, 对于一般的接收距离来讲, 这些并行线就相当于一个复合源, 等效于相同场地发射, 接收到的信号是复合的并行信号, 很难采用物理分隔的方法分别接收. 在时间上并行信号是同时发射, 无法采用时分方法进行接收; 在频率上, 又是以相同或相似的频率发射, 频谱分量相同或覆盖, 无法采用频分的方法接收. 因此串行信号的电磁泄漏问题仍是 TEMPEST 的重要课题之一^[31].

计算机等信息电子设备的电路一般都是由数字 PCB 实现的, 造成潜在的信息泄漏问题, 数字电路的驱动电流大, 辐射强度大, 高速的时钟脉冲和数字信号使得辐射频带加宽. 激励信号是参数各异的方波或梯形波, 以如图 2 所示梯形波 $f(t)$ 为例, 其幅值、周期、升降沿及脉宽分别为 I_0 , T , t_r , T_w .

图 3 传导泄漏

Figure 3 Conduction leakage

该激励信号可表示为 Fourier 级数的形式,

$$f(t) = \sum_{n=-\infty}^{\infty} F_n e^{jw_n t}, \quad (1)$$

其中

$$F_n = \frac{1}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} f(t) e^{-jw_n t} dt = \frac{I_0 T_w}{T} H(w_n T_w) H(w_n T_r), w_n = \frac{2n\pi}{T}, \quad (2)$$

$H(w_n T_w) = \sin(w_n T_w / 2) / w_n T_w / 2$, 因此得到其 Fourier 变换为

$$F(w) = \frac{1}{2\pi} \sum_{n=-\infty}^{\infty} F_n \int_{-\infty}^{\infty} e^{j(w_n - w)t} dt = \sum_{n=-\infty}^{\infty} F_n \delta(w - w_n). \quad (3)$$

可见周期梯形波信号的谱分布只有窄带谱, 分布于 $w = w_n$ 的频率点上. 除 $n = 0$ 外, 在 $w = w_n$ 的点上, $F(w)$ 的幅值为 F_n .

对于非周期信号, Fourier 变换对为

$$f(t) = \int_{-\infty}^{\infty} F(w) e^{jw t} dw, \quad (4)$$

$$F(w) = \lim_{T \rightarrow \infty} \frac{T}{2\pi} \int_{-\infty}^{\infty} F_n \delta(w' - w) dw' = \frac{I_0 T_w}{2\pi} H(w_n T_w) H(w_n T_r). \quad (5)$$

计算机系统中视频电缆传送的信号是串行信号, 驱动电流大、连线长度长、信息量大、暴露多、易于产生电磁辐射和信息泄漏, 并且其线度一般比波长和源场距离大, 因此建立其传输线模型. 对于多线电缆, 一般公用一根导线作为地线或者回流线, 因此 n 根导线组成的电缆可以看作 $(n-1)$ 对传输线, 整个电缆的辐射结果则为 $(n-1)$ 对传输线各自辐射结果的叠加^[31].

计算机等信息设备泄漏源的传导模型如图 3 所示, 传导发射泄漏是杂散电磁能量通过各种线路传导出去, 其中最大量和最基本的辐射源是载流导线. 辐射泄漏和传导泄漏相互关联, 存在相互能量交换现象, 沿线传导的杂散电磁能量可以因导线的天线效应部分的转化为电磁波辐射出去, 而且辐射到空间的杂散电磁能量又可因导线的天线效应耦合到外连导线上.

2.2 电源线传导泄漏

计算机系统的电源线、机房内的电话线等都可作为传导媒介, 电子信息设备的有用信号在电源线上感应信号而导致的传导泄漏为基于电源线的传导泄漏, 它包括计算机的辐射泄漏在电源线中产生的感应电流和计算机本身线路传导电流. 基于电源线的传导泄漏模型如图 4 所示.

图 4 基于电源线传导泄漏

Figure 4 Conduction leakage based on power line

计算机等信息设备辐射产生电磁波, 具有不断变化的电场和不断变化的磁场, 根据 Faraday 电磁感应定律, 磁场耦合在信息设备的电源导线回路上产生感应电动势

$$\varepsilon_{Bin} = -\frac{d\phi}{dt} = -\frac{d}{dt} \int_S B \cdot dS. \quad (6)$$

进而产生感应电流, 由 I_{Bin} 表示.

计算机信息设备的视频信号线与电源线之间除了产生上述磁场感应电流之外, 同时由于高频作用会产生电场耦合, 从而在电源线上产生信号电流, 由 I_{Ein} 表示. 因此电源线上的感应电流可表示为

$$I_{induce} = I_{Bin} + I_{Ein}. \quad (7)$$

上述感应电流与计算机线路传导电流 $I_{conduction}$ 一起构成了计算机电源线上传导的信号电流:

$$I = I_{conduction} + I_{induce}. \quad (8)$$

携带有计算机等信息设备信息的电流信号通过接线板在电源线中传输, 甚至在电源网中传输, 在具有一定的信号完整性的条件下, 利用特定的侦收设备, 可实现对传导泄漏信息的接收和还原, 从而导致有用信息的泄漏.

2.3 电源线辐射泄漏

由上小节分析可知, 电源线中的传导电流 I 携带计算机等信息设备的信息, 根据 Maxwell 电磁理论, 变化的电场产生磁场, 电源线的传导电流在电源线周围产生变化的磁场, 变化的磁场产生电场, 相互作用的电场和磁场使得电源线周围产生携带计算机等信息设备信息的电磁波. 电源线电磁辐射模型为电缆的辐射泄漏模型, 利用泄漏源辐射问题中的传输线辐射分析方法, 在相同条件下, 同样适用于电源线电缆的辐射问题.

基于电源线的电磁泄漏示意模型如图 5 所示, 并且随着电源线通信技术的发展, 利用电源线进行信息传输和信息交换, 不可避免的产生信息辐射泄漏, 因此基于电源线的电磁信息泄漏问题, 将会给信息安全带来巨大的潜在威胁.

2.4 双电流探头测试方法

该方法使用信号源发生器产生信号电流, 这个信号电流代表泄漏信号在电源线上传输, 通过电流注入探头将该信号注入到电源线中, 由检测式输出电流探头从电源线中检测信号电流. 测试平台配置

图5 基于电源线电磁泄漏示意模型

Figure 5 Model of electromagnetic leakage based on power line

图6 双电流探头测试

Figure 6 Double current probes measurement

图7 电流探头等效电路

Figure 7 Equivalent circuit of current probe

如图6所示,一个电流探头作为信号电流注入,另一个作为频谱仪接收信号电流的接收探头,通过频谱仪读出输出电流探头所接收到的电压。

电流探头为一个分成两半的高磁导率磁芯,被测电流穿过探头,在磁芯的线圈上感应电压,通过连接器连接输出至频谱仪。电流探头等效电路如图7所示。 M 为电流探头与被测电源线的互感, L_1 为穿过电流探头的被测电源线的自感, L 为电流探头绕线的自感, C 为分布电容, r 为电流探头绕线电阻, R 为仪器内阻(一般为 $50\ \Omega$), V_o 为输出电压, Z 为虚线内的总电阻。运用电路原理,得

$$j\omega MI_1 = j\omega LI_2 + ZI_2, \quad (9)$$

$$Z = \frac{R + r}{1 + j\omega C(R + r)}, \quad (10)$$

$$I_2 = \frac{j\omega MI_1}{Z + j\omega L}, \quad (11)$$

$$V_o = \frac{j\omega MI_1}{Z + j\omega L} Z \frac{R}{R + r}, \quad (12)$$

图 8 输出电压与频率的关系

Figure 8 Relation between output voltage and frequency

图 9 双探头测试等效电路

Figure 9 Equivalent circuit of double probes measurement

$$Z_t = \frac{V_o}{I_1} = \frac{j\omega MR}{(R+r)(1-\omega^2 LC) + j\omega L}. \quad (13)$$

可见传输阻抗与 M , R , L , C , r 及频率均有关系, 逐个分析电感、电容及内阻对电路的影响, 可得出输出电压与频率的关系如图 8 所示. 其中 $f_0 = R/2\pi L$, $f_1 = 1/2\pi\sqrt{LC}$, 分布电容 C 一般较小, 因此 $f_0 < f_1$. 电感越大, 平坦区越往左, 低频特性越好, 而分布电容影响电流卡钳的高频区域, 分布电容越小, 高频特性越好.

基于双探头测试的等效电路如图 9 所示, V_i 为信号源注入电压, R_i 为信号源内阻, Z 为传输线阻抗, V_o 为输出电压, R 为接收仪器内阻. 设注入电流探头插入损耗为 I_{nl} , 输出电流探头传输阻抗为 Z_t , 不考虑传输线阻抗, 可得注入功率 $P_{in} = V_i - I_{nl}$, 设电源线传输阻抗为 r , 并根据式 (13) 输出电压和输入电压的关系, 可得输出电压为

$$V_o = V_i - 17 - I_{nl} - 10\lg r + 20\lg Z_t. \quad (14)$$

3 基于电源线电磁泄漏实验验证与分析

3.1 基于通用仪器电源线电磁泄漏实验验证

基于通用仪器的电源线电磁泄漏实验图如图 10 所示, 在实验室场景下, 由信号发生器产生红信号, 利用电流钳 (注入电流钳) 将该信号注入与插座 1 相连的电源线中, 同时利用电流钳 (输出电流钳) 获取与插座 2 相连的电源线上的传输信号, 并通过频谱仪作为接收机接收该信号.

图 10 实验图

Figure 10 Experiment platform

图 11 输入信号参数设置

Figure 11 Parameters of input signal

图 12 接收还原红信号频谱图

Figure 12 Spectrum of received red signal

实验中需保证插座 1 和 2 位于同一电源网中, 信号发生器产生的输入红信号参数设置如图 11 所示, 即产生中心频率为 50 MHz、幅度为 15 dBm、脉宽为 8 μ s、周期为 16 μ s、占空比为 50% 的脉冲信号。注入电流钳频率范围为 2 ~ 400 MHz, 输出电流钳的频率范围为 1 MHz ~ 1 GHz。

频谱仪接收得到的红信号频谱图如图 12 所示, 可以看到该频谱具有离散型、谐波性和收敛性, 根据 Fourier 变换相关知识可知, 该接收信号是中心频率为 50 MHz、脉宽为 8 μ s、周期为 16 μ s 的周期脉冲信号, 与注入红信号参数一致。该实验验证了泄漏红信号可在同一电源网络的电源线中传输, 从而产生基于电源线的信号泄漏问题。

3.2 屏蔽暗室实验分析

3.1 小节对电源线传导泄漏进行了定性分析, 本小节在屏蔽暗室环境下对电源线传导泄漏进行定量实验分析。实验场景如图 13 所示。电源线、电流注入探头和输出电流探头置于暗室内, 两电流探头相距 2 m, 在控制室内连接信号源和频谱仪, 用于信号注入和接收。

信号源产生中心频率为 50 MHz、幅度为 112 dB μ V、脉宽为 8 μ s、周期为 16 μ s、占空比为 50% 的脉冲信号, 如图 14 所示。电流注入探头和输出电流探头的参数分别如表 1 和 2 所示。分别利用两种不同的注入和输出电流探头, 在相同注入信号条件下以及不同注入信号电压条件下, 定量测试输出

图 13 暗室实验场景

Figure 13 Experiment scene in anechoic chamber

图 14 注入信号参数设置

Figure 14 Parameters of injection signal

表 1 注入探头参数

Table 1 Injection probe parameters

Model number	9120-1N SOLAR ELECTRONICS	9144-1N SOLAR ELECTRONICS
Megnetic ring diameter	1.6 cm	1.9 cm
Frequency range	5 MHz ~ 1 GHz	10 kHz ~ 100 MHz
Insertion loss	10 dB	15 dB

表 2 输出探头参数

Table 2 Output probe parameters

Model number	9119-1N SOLAR ELECTRONICS	9215-1N SOLAR ELECTRONICS
Megnetic ring diameter	1.6 cm	1.6 cm
Frequency range	1 MHz ~ 1.2 GHz	20 Hz ~ 500 MHz
Transmission characteristic impedance	7	5

表 3 不同注入输出电流探头输出电压结果

Table 3 Output voltage result with different injection and output current probes

Measurement voltage (dBμV)		Injection current probe			
		9120-1N		9144-1N	
Output current probe	9119-1N	Measurement voltage60.46	Calculate voltage84.91	Measurement voltage54.03	Calculate voltage79.91
	9215-1N	Measurement voltage63.52	Calculate voltage81.99	Measurement voltage57.10	Calculate voltage76.99

信号电压. 频谱仪接收得到的红信号频谱特点与图 12 一致. 分别记录不同条件下接收信号频谱最大电压值, 如表 3 中的测试电压所示.

图 15 (网络版彩图) 输出电压随传输阻抗的变化

Figure 15 (Color online) The change of output voltage with transmission impedance

图 16 (网络版彩图) 输出电压与注入电压的关系

Figure 16 (Color online) Relation between output and injection voltage

结合理论分析以及电流探头参数, 当电流注入探头为 9120-1N 时, 插入损耗为 10 dB; 当电流注入探头为 9144-1N 时, 插入损耗为 15 dB; 当输出电流探头为 9119-1N 时, 传输特性阻抗为 7 Ω ; 当输出电流探头为 9215-1N 时, 传输特性阻抗为 5 Ω . 依据电流探头特性阻抗和输出电压的关系, 设电源线传输阻抗为 50 Ω 时, 分别计算表 3 四种情况下的输出电压值, 比较实测值和计算求解值, 测试电压比计算电压约小 20 dB μ V, 其误差来源主要为信号传输线阻抗、电流探头实际参数与理论值的偏差, 其中计算中所取输出电流探头的传输特性阻抗为最大值, 当考虑输出电流探头 9119-1N 的传输特性阻抗在 1 ~ 7 Ω 变化, 9215-1N 的传输特性阻抗在 1 ~ 5 Ω 变化, 输出电压 V_o 随传输特性阻抗 Z_t 的变化如图 15 所示, 电流注入探头为 9120-1N 时, 输出电压值在 68.01 ~ 84.91 dB μ V 之间; 电流注入探头为 9144-1N 时, 输出电压值在 63.01 ~ 79.91 dB μ V 之间.

当注入不同幅度的信号时, 电流注入探头为 9120-1N, 输出电流探头为 9119-1N, 得到的测试结果如图 16 所示, 可见输出电压与注入电压近似为线性关系.

3.3 计算机视频信息电源线电磁泄漏分析

本小节对台式计算机视频信息的电源线泄漏进行实验验证分析, 实验所需设备为被测台式计算机 (联想开天 M6900)、显示器 (Hp VS17e EN623NN)、普通视频电缆连接线、多个接线板电源线、示波器、处理用计算机、电流钳、实验场景图 (如图 17 所示), 利用多个接线板串联, 并与被测台式计算机的接线板相连, 形成约 20 m 的电源线, 电流钳分别在以 2 m 为间隔的位置获取泄漏信号, 共获取 10 个位置的信号, 利用示波器作为接收设备接收泄漏数据供计算机处理.

被测台式计算机处于打开状态, 并打开 word 文档, 显示器显示如图 18 所示, 利用电流钳获取电源线传导信号, 并由示波器接收存储, 其中 2 m 处的信号如图 19 所示, 在电源线每个位置处获取的信号能量最大值如图 20 所示, 由图可见, 随着电源线长度的增加, 泄漏信号的能量稍有下降, 但下降缓慢. 由计算机处理得到的每个位置处一帧视频还原结果 (如图 21 所示) 可以看到, 电源线长度较小, 即距被测台式计算机较近时, 接收视频信号的效果反而较差, 主要原因是计算机系统辐射和传导的复杂性, 计算机辐射和传导泄漏在近距离的能量均较强, 因此对视频信号的接收和还原存在较多的其他干扰, 而在距离大于 10 m 后, 视频信号处理效果更好.

图 17 (网络版彩图) 实验场景
Figure 17 (Color online) Experiment scene

图 18 (网络版彩图) 视频显示
Figure 18 (Color online) Video display

图 19 (网络版彩图) 一帧视频信号
Figure 19 (Color online) One frame video signal

图 20 (网络版彩图) 最大值曲线
Figure 20 (Color online) Maximum curve

由本实验可见, 基于电源线的电磁信息泄漏, 特别是串行视频信号的泄漏可以长距离传输, 并可通过一定的接收处理, 实现对泄漏信号的还原, 因此对信息安全具有较大的危害性.

图 21 视频还原图

Figure 21 Video reconstruction. (a) 2 m; (b) 4 m; (c) 6 m; (d) 8 m; (e) 10 m; (f) 12 m; (g) 14 m; (h) 16 m; (i) 18 m; (j) 20 m

4 小结

本文针对基于电源线的电磁泄漏问题, 从泄漏的原理、模型、仿真以及实验上展开了分析和研究, 研究了计算机信息设备的泄漏机理, 建立了基于电源线的信号传导辐射泄漏模型, 在实验室条件下对电源线信息泄漏进行了实验验证和分析, 验证了基于电源线的电磁信息泄漏给信息安全带来的潜在威胁. 我国对 TEMPEST 技术的研究起步较晚, 国外技术对我国保密, 并且缺乏必要的技术支持和系统研究, 许多课题有待深入与扩展, 后续将进一步分析电源线电磁信息泄漏的影响因素, 突破微弱信号检测、红黑信号鉴别、信息侦收和还原等关键技术, 实现电源线电磁泄漏信号的检测、分析、接收和还原.

参考文献

- 1 van Eck W. Electromagnetic radiation from video display units: an eavesdropping risk. *Comput Secur*, 1985, 4: 269–286
- 2 Highland H J. TEMPEST over leaking computer. *Comput Secur*, 1988, 13: 457–458
- 3 Szilagyi A, Nicolaescu I. Evaluation of the compromising radiation by electromagnetic compatibility tests. In: *International Conference on Communications*. Bucharest: IEEE Press, 2012. 143–145
- 4 Elibol F, Sarac U, Erer I. Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system. In: *Proceedings of the 20th European Signal Processing Conference*. Bucharest Romania: IEEE Press, 2012. 1767–1771
- 5 Auddy A, Sahu S. Tempest: magnitude of threat and mitigation techniques. In: *10th International Conference on Electromagnetic Interference Compatibility*. Bangalore: IEEE Press, 2008. 603–611
- 6 Suzuki Y, Akiyama Y. Jamming technique to prevent information leakage caused by unintentional emissions of PC video signals. In: *IEEE International Symposium on Electromagnetic Compatibility*. Fort Lauderdale: IEEE Press, 2010. 132–137
- 7 Degauque P, Laly P, Degardin V, et al. Compromising electromagnetic field radiated by in-house PLC lines. In: *IEEE Global Telecommunications Conference*. Miami: IEEE Press, 2010. 1–5
- 8 Degauque P, Laly P, Degardin V, et al. Power line communication and compromising radiated emission. In: *International Conference on Software, Telecommunications and Computer Networks, Dalmatia*, 2010. 88–91
- 9 Hayashi Y, Homma N, Mizuki T, et al. Efficient evaluation of EM radiation associated with information leakage from cryptographic devices. *IEEE Trans Electromagn Compat*, 2013, 55: 555–563
- 10 Hayashi Y, Homma N, Mizuki T, et al. Transient IEMI threats for cryptographic devices. *IEEE Trans Electromagn Compat*, 2013, 55: 140–148
- 11 He B, Wang J Z, He D, et al. Study on EM-side channel test for embedded system. In: *International Conference on Computer Science and Network Technology*, Harbin, 2011. 2368–2371
- 12 Todri A, Marek-Sadowska M. Reliability analysis and optimization of power-gated ICs. *IEEE Trans VLSI Syst*, 2011, 19: 457–468
- 13 Hayashi Y I, Homma N, Watanabe T, et al. Introduction to the special section on electromagnetic information security. *IEEE Trans Electromagn Compat*, 2013, 55: 539–546
- 14 Bindar V, Popescu M, Vulpe A. Considerations regarding shielding effectiveness and testing of electromagnetic protected enclosures used in communications security. In: *10th International Conference on Communications*, Sydney, 2014. 1–6

- 15 Zajic A, Prvulovic M. Experimental demonstration of electromagnetic information leakage from modern processor-memory systems. *IEEE Trans Electromagn Compat*, 2014, 56: 885–893
- 16 Chen Z M, Sinha A, Schaumont P. Using virtual secure circuit to protect embedded software from side-channel attacks. *IEEE Trans Comput*, 2013, 62: 124–136
- 17 Soll O, Korak T, Muehlberghuber M. EM-based detection of hardware trojans on FPGAs. In: *IEEE International Symposium on Hardware-Oriented Security and Trust*, Arlington, 2014. 84–87
- 18 Zhou C L, Zhang H L, Yu Q, et al. The impact of electromagnetic security on computer systems and networks. In: *IEEE 3rd International Conference on Communication Software and Networks*. Xian: IEEE Press, 2011. 56–59
- 19 Xiang C B, Xu J H. A method to extract the synchronous characters in the electromagnetic information leaked by a computer. In: *4th International Congress on Image and Signal Processing*, Shanghai, 2011. 2630–2633
- 20 Zhu D L, He P, Zhang J Q. Research of key problem of receiving and recovery of signal based on wide band receiver. In: *International Conference on Internet Technology and Applications*, Wuhan, 2010. 1–8
- 21 Liu D X, Guo W L. Principle analysis of computer information leakage. *J XiDian Univ*, 1993, 2: 74–79 [刘德修, 郭万里. 计算机信息泄漏的机理分析. 西安电子科技大学学报, 1993, 2: 74–79]
- 22 Zhang D W, Sun L, Zhang H Y. Research on TEMPEST technology of computer system. *Modern Electron Tech*, 2011, 34: 88–97 [张大为, 孙雷, 张海鹰. 计算机系统的 TEMPEST 技术研究. 现代电子技术, 2011, 34: 88–97]
- 23 Chen R M, Ren J C, Gong Z H. Research on Soft-TEMPEST technology for monitor electromagnetic Trojans. *Comput Eng Appl*, 2012, 48: 63–68 [陈荣茂, 任江春, 龚正虎. 显示器电磁木马的 Soft-TEMPEST 技术研究. 计算机工程与应用, 2012, 48: 63–68]
- 24 Dong N. Research on electromagentic leakage emanations of USB keyboard. Dissertation for M.S. Degree. Beijing: Beijing University of Posts and Telecommunication, 2012 [董宁. USB 键盘信息电磁泄漏的测试、仿真及防护技术研究. 硕士学位论文. 北京: 北京邮电大学, 2012]
- 25 Chen X G. Study on detection method of weak leakage electromagnetic signal for digital system. Dissertation for Ph.D. Degree. Wuhan: Huazhong University of Science and Technology, 2012 [陈新国. 数字系统微弱泄漏电磁波信号检测方法研究. 博士学位论文. 武汉: 华中科技大学, 2012]
- 26 Shi S, Liu T K, Jiang Y. Based on red and black signal on the host computer for testing and analysis of electromagnetic leakage. *Comput Secur*, 2011, 1: 44–46 [石森, 刘泰康, 姜云. 基于红黑信号的计算机主机电磁泄漏的测试与分析. 计算机安全, 2011, 1: 44–46]
- 27 Chen K Y, Zhang P, Deng G M, et al. Electromagnetic correlation attacks and the minimum number of attack traces analyzing. *J Huazhong Univ Sci Technol*, 2011, 39: 32–35 [陈开颜, 张鹏, 邓高明, 等. 相关性电磁分析攻击及最小样本量分析. 华中科技大学学报, 2011, 39: 32–35]
- 28 Yang W H, Lv Y H. Analysis of information recovery from EM leakage of computers. *J Beijing Univ Posts Telecommun*, 2011, 34: 26–29 [杨文翰, 吕英华. 计算机电磁辐射信息再现分析. 北京邮电大学学报, 2011, 34: 26–29]
- 29 Zhang P, Zhou C, Deng G M, et al. A hardware trojans design using the correlation analysis of electromagnetic emanation. *J Huazhong Univ Sci Technol*, 2010, 38: 22–25 [张鹏, 邹程, 邓高明, 等. 基于电磁泄漏相关性分析的硬件木马设计. 华中科技大学学报, 2010, 38: 22–25]
- 30 Zhou K J, Zhao G. Principle of Electromagnetic Compatibility. Harbin: Harbin Engineering University Press, 2003 [周开基, 赵刚. 电磁兼容性原理. 哈尔滨: 哈尔滨工程大学出版社, 2003]
- 31 Han F. Computer Information Electromagnetic Leakage and Protection. Beijing: Science Press, 1993 [韩放. 计算机信息电磁泄漏与防护. 北京: 科学出版社, 1993]

Modeling and experimental research on electromagnetic information leakage from power lines

XU YanYun, HUANG WeiQing*, FAN Wei, ZHANG Meng & WEI Dong

Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

*E-mail: huangweiqing@iie.ac.cn

Abstract The problem of information security is increasingly prominent with the ongoing development of information technology. Electromagnetic (EM) information leakage is a great hidden danger to information security, and research on the topic has great significance. In this paper, the principle of power line (PL) EM information leakage in computers is studied. PL conduction and radiation leakage models are built. Experimental analysis is implemented to further prove the potential harmfulness to security of EM information leakage from PL.

Keywords information security, electromagnetic security, compromising emanation, electromagnetic information leakage, conduction leakage, radiation leakage

XU YanYun was born in 1985. She received her B.E. degree from the Ocean University of China, Qingdao, China, in 2007. She received her Ph.D. degree from the Institute of Electronics, Chinese Academy of Sciences, Beijing, China, in 2012. Since 2012, she has been working with the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. Her research interests include electro-

magnetic information security, signal processing, weak signal detection, and ultra-wideband radar detection.

HUANG WeiQing was born in 1972. He received his B.E. degree from Beijing University of Technology in 1994 and his M.S. degree from the Beijing University of Posts and Telecommunications in 2002. Since 2012, he has been working with the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China, where he is the fourth laboratory director. His research interests include wireless communication security, electromagnetic signal processing,

network security technology, Internet-of-Things security, and cloud computing security technology.